# ÁLGEBRA MODERNA

Hygino H. Domingues
Gelson Iezzi

Hygino H. Domingues
Gelson Iezzi

# ÁLGEBRA MODERNA

**4ª edição reformulada**

# APRESENTAÇÃO

O presente trabalho é uma nova versão, bastante reformulada e com algumas ampliações, de *Álgebra moderna*, dos mesmos autores. Dois motivos principalmente levaram a essas mudanças: de um lado a constatação de um certo desgaste da versão anterior, no que se refere à redação e à abordagem, inevitável quando se considera o tempo há que a obra está em circulação — cerca de duas décadas e meia — e que ela foi escrita ainda sob alguma influência da corrente da *matemática moderna;* de outro, o fato de ter alcançado e mantido, ao longo desse tempo, uma boa aceitação por parte de estudantes e professores de cursos de matemática, comprovada pelas várias edições e reimpressões alcançadas durante esses anos.

Levando em conta o primeiro desses motivos, o livro foi totalmente reescrito, numa linguagem muito menos permeada de simbolismos que a das edições anteriores, com vistas a tornar a leitura mais leve e agradável, e com muito mais exemplos e ilustrações. Procurou-se também, na medida do possível, evitar a iniciação a um dado assunto sem algum comentário ou observação inicial que pudesse servir de motivação para seu estudo. Também a título de motivação, todos os capítulos apresentam notas e/ou observações históricas referentes às origens de alguns dos tópicos tratados, importantes, ao nosso ver, em face do caráter abstrato da álgebra moderna. Não se tratando de obra que prioriza as aplicações, até pelo seu caráter introdutório, busca-se, com essas notas e/ou observações, mostrar de onde vem a álgebra moderna, o que pode constituir uma pista importante para o leitor vislumbrar a origem e o alcance de alguns dos métodos desse campo da matemática.

Efetivamente, apenas um dos tópicos focalizados na presente edição não figurava, de alguma maneira, nas anteriores: aquele contemplado no capítulo I com o título *Noções sobre conjuntos e demonstrações*. Talvez desnecessário quando da primeira redação, esse tópico nos parece muito importante na presente conjuntura das licenciaturas em matemática, área para a qual se destina principalmente a obra. De fato, apesar de ser bastante moderado no uso do formalismo matemático, o livro faz um estudo sistemático do assunto alvo e, portanto, compreende um número considerável de teoremas e respectivas demonstrações. Ora, é bem sabido que hoje poucos alunos chegam à universidade com alguma experiência em demonstrações e que essa lacuna às vezes não é preenchida antes de iniciarem um curso de álgebra. Mas não se vai no assunto, nesse capítulo, além do mínimo necessário como pré-requisito para um entendimento suficiente do método matemático e a abordagem é propositadamente despretensiosa e informal.

O capítulo II, *Introdução à aritmética dos números inteiros*, sofreu dois tipos de alterações em relação às edições anteriores: além de ter sido ampliado com um estudo das equações diofantinas lineares de primeiro grau, em duas incógnitas, e do problema chinês do resto, recebeu na presente versão uma abordagem mais pormenorizada e mais rica em exemplos e aplicações. Sem falar no seu papel como pré-requisito para os capítulos que o seguem, a ênfase maior dada a esse tópico deriva de duas razões que se integram: (i) a importância crescente de suas aplicações — na criptografia, por exemplo; (ii) o fato de o assunto muitas vezes ser ignorado nos cursos de matemática, com prejuízo considerável para a formação dos futuros professores e pesquisadores.

Como nas edições anteriores, o capítulo III, *Relações, aplicações, operações,* é muito esmiuçado, abundante em detalhes, talvez mais do que nenhum dos outros, porque, além de também ser um dos pré-requisitos básicos para os capítulos centrais do livro, envolve assuntos que fazem parte do ensino de matemática no ciclo básico que cumpre valorizar por si mesmos e ajustar às necessidades do desenvolvimento da matéria.

Os capítulos IV e V focalizam, respectivamente, a teoria básica das estruturas algébricas de grupo e anel (com seus subcasos mais importantes). O capítulo IV, *Grupos,* além das mudanças de caráter geral já mencionadas no que se refere à linguagem e abordagem, com ênfase maior nos exemplos, apresenta como novidade um estudo mais abrangente e sistemático dos grupos de permutações. Quanto ao capítulo V, *Anéis e corpos,* houve a incorporação do tópico destinado ao estudo da compatibilidade de uma relação de ordem com a estrutura de anel, que na versão anterior constituía um capítulo à parte.

O capítulo VI, *Anéis de polinômios,* foi totalmente reformulado. Nas edições anteriores, introduzia-se o conceito de polinômio sobre um anel como uma seqüência quase-nula de elementos desse anel. Essa definição, se tem a vantagem da generalidade, e até de proporcionar uma certa facilidade algébrica para desenvolver a teoria que segue, tem o inconveniente, para quem está iniciando o estudo do assunto, de ser muito artificiosa. Preferimos, considerando o objetivo da obra, definir *polinômio* sobre um anel de integridade infinito como uma aplicação (função polinomial) e depois, considerando a hipótese feita sobre o anel, provar e explorar o princípio de identidade de polinômios.

Entre as propostas da obra, uma era a de incluir um tópico final que, digamos assim, fugisse um pouco ao "básico". Inúmeras escolhas poderiam ser feitas. Mas optamos por *Anéis principais e fatoriais,* título do capítulo VII, considerando tratar-se de uma generalização natural da teoria da divisibilidade no anel dos inteiros, que, por isso mesmo, não exige muito em termos de conceitos novos mas, não obstante, dá uma boa idéia inicial do alcance dos métodos da álgebra moderna.

No que se refere à redação do livro, o trabalho foi dividido entre os autores da seguinte maneira:

**Professor Hygino H. Domingues**

- Toda a teoria e exemplos dos capítulos I, II, IV, V, VI e VII.
- Os exercícios, propostos e resolvidos, dos capítulos I e II, inclusive respostas.
- Todas as notas históricas.

**Professor Gelson Iezzi**

- Toda a teoria e exemplos do capítulo III, em parceria com o professor Hygino.
- Os exercícios, propostos e resolvidos, dos capítulos III, IV, V, VI e VII, inclusive respostas.

Finalmente, nossos agradecimentos a todos os colegas que usaram a obra em suas edições anteriores, especialmente os da PUC-SP e Unesp de São José do Rio Preto, com os quais compartilhamos o uso desse material por certo tempo e que, com seus comentários eventuais, nos deram algumas pistas para as mudanças presentes.

Os autores

# SUMÁRIO

CAPÍTULO I

# NOÇÕES SOBRE CONJUNTOS E DEMONSTRAÇÕES

## I–1 SOBRE CONJUNTOS

### 1. NOTA HISTÓRICA

A teoria dos conjuntos foi criada por G. Cantor (1845-1918), com uma série de artigos publicados a partir de 1874. Embora russo de nascimento, Cantor fez carreira na Alemanha, para onde sua família se mudara quando ele era criança. Depois de doutorar-se na Universidade de Berlim, em 1867, com uma tese sobre teorla dos números, passou a trabalhar na Universidade de Halle, onde ficaria até o fim de sua carreira acadêmica.

Por volta de 1870, quando estudava o problema da representação das funções reais por meio de séries trigonométricas, sua atenção se voltou para uma questão com a qual seu espírito tinha uma afinidade natural muito grande: a natureza do infinito. Esse foi o ponto de partida da criação da teoria dos conjuntos.

Além de tudo, os trabalhos de Cantor sobre teoria dos conjuntos exigiram uma boa dose de coragem científica. De fato, ao estender a idéia de "cardinal" para conjuntos infinitos[1], Cantor estava considerando a infinitude destes como algo efetivamente atual e não apenas potencial, como se aceitava até então.

[1] Diz-se que dois conjuntos têm o mesmo "cardinal" ou a mesma "cardinalidade" se seus elementos podem ser postos em correspondência biunívoca.

O grande mérito de Cantor foi perceber a existência de uma hierarquia para os cardinais transfinitos. Assim, todos os conjuntos cujos elementos podem ser postos em correspondência biunívoca com os elementos do conjunto dos números naturais têm o mesmo e o "menor" cardinal transfinito. Trata-se dos *conjuntos enumeráveis*. Entre estes encontram-se, por exemplo, o conjunto dos números inteiros e, surpreendentemente, o conjunto dos números racionais. Cantor, mostrou ainda que o conjunto dos números reais tem cardinal "maior" que o dos conjuntos enumeráveis e que esse cardinal é "igual" ao do conjunto dos irracionais, algo que contrariava a velha idéia de que o todo tinha de ser maior que a parte. E mostrou que a escala dos cardinais transfinitos não tem limite: sempre há cardinais "maiores" e "maiores".

Tão surpreendentes eram alguns dos resultados encontrados por Cantor que ele chegou a dizer sobre um deles: "Vejo, mas não acredito". Assim, não é de espantar o fato de que grandes matemáticos tenham rejeitado seus trabalhos. L. Kronecker (1823-1891) chegou a chamar Cantor de charlatão da ciência. E até havia razão para algumas dessas críticas, pois construída inicialmente sem preocupações com seus fundamentos lógicos, a teoria dos conjuntos, antes de ser satisfatoriamente axiomatizada no século XX, gerou paradoxos que chegaram a confundir e inquietar os matemáticos, até mesmo os "cantoristas".

Mas, para o progresso da matemática, prevaleceram opiniões como a de B. Russel (1872-1970), que considerava a teoria dos conjuntos como "provavelmente a mais importante [descoberta] que a época pode ostentar" ou a de D. Hilbert (1862-1943), que disse: "Do paraíso criado por Cantor ninguém nos tirará".

## 2. CONJUNTOS

### 2.1 Introdução

O conceito de *conjunto* é certamente um dos mais importantes da matemática contemporânea. Como sinônimo de conjunto, no sentido aqui considerado, poderemos usar sem distinção os termos "classe" e "coleção". Um conjunto é formado por objetos, de modo genérico chamados de *elementos*, que, por um motivo ou outro, convém considerar globalmente. Não há restrições quanto à escolha dos elementos de um conjunto, salvo que excluiremos a possibilidade de um conjunto ser elemento dele mesmo. Assim, não há nenhum inconveniente em considerar, por exemplo, um conjunto formado por um número real, uma bola de futebol e um automóvel.

Costuma-se indicar os conjuntos por letras maiúsculas e seus elementos por letras minúsculas de nosso alfabeto. Se um objeto $a$ é elemento de um conjunto $U$, dizemos que "$a$ pertence a $U$" e denotamos essa relação por $a \in U$. Caso contrário, dizemos que "$a$ não pertence a $U$" e escrevemos $a \notin U$.

## 2.2 Descrição de um conjunto

Comumente usam-se três procedimentos para definir um conjunto.

- Descrever seus elementos por uma sentença. Por exemplo:

— conjunto dos números reais;

— conjunto dos planetas do sistema solar.

- Listar seus elementos entre chaves. Por exemplo:

$\{2, 4, 6, 8, 10\}$

$\{0, 1, 2, 3, ...\}$

(No segundo exemplo, como se vê, só os três primeiros elementos foram listados, mas mesmo assim não há dúvida de que se trata do conjunto dos números naturais.)

- Dar uma "propriedade" que identifica seus elementos. Por exemplo:

$\{x \mid x$ é inteiro e $x > 2\}$

$\{x \mid x$ é real e $2 < x < 10\}$

$\{x \mid x$ goza da propriedade $P\}$

A propósito do último procedimento, vale ressaltar que um dos pontos importantes do uso de conjuntos na matemática reside no fato de estes poderem substituir as propriedades com grande vantagem no que se refere à precisão de linguagem. Por exemplo, a propriedade "Todos os números racionais são também números reais", na linguagem de conjuntos, pode ser escrita assim: "Se $x \in \mathbb{Q}$, então $x \in \mathbb{R}$". (Ver notação abaixo.)

Certos conjuntos, por sua importância e pela freqüência com que se repetem, são indicados por notações especiais:

$\mathbb{N} = \{0, 1, 2, 3, ...\}$ (conjunto dos números naturais);

$\mathbb{Z} = \{..., -2, -1, 0, +1, +2, ...\}$ (conjunto dos números inteiros);

$\mathbb{Q}$ = conjunto dos números racionais;

$\mathbb{R}$ = conjunto dos números reais.

Se $A$ indica um dos três últimos conjuntos, indistintamente, então:

$A^* = A - \{0\}$

$A_+ = \{x \in A \mid x \geqslant 0\}$ (conjunto dos números positivos de $A$)

$A_- = \{x \in A \mid x \leqslant 0\}$ (conjunto dos números negativos de $A$)

$A_+^* = \{x \in A \mid x > 0\}$ (conjunto dos números estritamente positivos de $A$)

$A_-^* = \{x \in A \mid x < 0\}$ (conjunto dos números estritamente negativos de $A$)

$\mathbb{C}$ = conjunto dos números complexos

$\mathbb{C}^* = \mathbb{C} - \{0\}$

## 2.3 Subconjuntos

Se $A$ e $B$ são conjuntos e todo elemento de $A$ também é elemento de $B$, dizemos que $A$ é um *subconjunto* de $B$ ou uma *parte* de $B$ e denotamos essa relação por

$A \subset B$ (lê-se "$A$ está contido em $B$") ou $B \supset A$ (lê-se "$B$ contém $A$") Dois conjuntos, $A$ e $B$, dizem se *iguais* se $A \subset B$ e $B \subset A$ (evidentemente isso significa que os dois conjuntos constam exatamente dos mesmos elementos). A igualdade de conjuntos é denotada pelo símbolo usual de igualdade. Por exemplo, se $A \quad \{x \in \mathbb{Z} \mid 1 < x < 5\}$ e $B \quad \{2, 3, 4\}$, então $A = B$.

A relação definida por $X \subset Y$, chamada *inclusão*, goza das seguintes propriedades:

- *reflexiva*: $X \subset X$;
- *anti-simétrica*: se $X \subset Y$ e $Y \subset X$, então $X = Y$;
- *transitiva*: se $X \subset Y$ e $Y \subset Z$, então $X \subset Z$.

A demonstração da primeira dessas propriedades é imediata. A segunda propriedade é decorrência da própria definição de igualdade de conjuntos. Para provar a terceira, temos de mostrar que todo elemento de $X$ também é elemento de $Z$. Ora, se $a \in X$, então $a \in Y$, por hipótese; mas, pertencendo a $Y$, $a$ também pertence a $Z$, pela segunda parte da hipótese; isso prova a propriedade.

O exemplo seguinte ilustra o uso da transitividade na linguagem de conjuntos. Indiquemos por $M$, $N$ e $S$, respectivamente, o conjunto dos quadriláteros, dos retângulos e dos quadrados de um dado plano. Como $S \subset N$ (todo quadrado é um retângulo) e $N \subset M$ (todo retângulo é um quadrilátero), então $S \subset M$.

Convém ressaltar que são equivalentes as três afirmações que seguem:

- $A \subset B$
- Se $x \in A$, então $x \in B$.
- Se $x \notin B$, então $x \notin A$.

Se $A$ e $B$ indicam conjuntos tais que $A \subset B$ e $A \neq B$, diz-se que $A$ está contido *propriamente* em $B$ ou que $B$ contém *propriamente* $A$. As notações usadas para indicar essas relações são, respectivamente, $A \subsetneqq B$ e $B \supsetneqq A$.

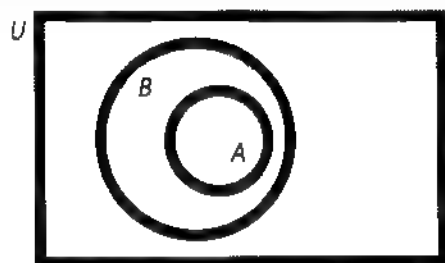
Por exemplo, o conjunto dos números naturais está contido propriamente no conjunto dos números inteiros, ou seja, $\mathbb{N} \subsetneqq \mathbb{Z}$. Ou, dito da outra forma: o conjunto dos números inteiros contém propriamente o conjunto dos números naturais, ou seja, $\mathbb{Z} \supsetneqq \mathbb{N}$.

## 2.4 Conjunto vazio

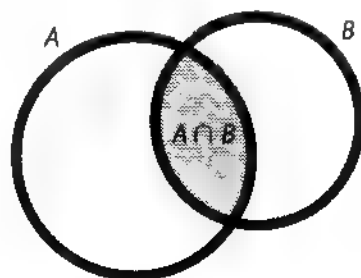
Com vistas a poder lidar com a linguagem de conjuntos mais uniformemente, aceita se a existência de um "conjunto sem elementos": o *conjunto vazio*, que pode ser definido por qualquer propriedade contraditória e que é denotado pelo símbolo $\varnothing$. Por exemplo: $\varnothing = \{x \in \mathbb{Q} \mid x \notin \mathbb{R}\}$. Uma decorrência lógica (mas estranha) da aceitaçao da existência de conjunto vazio é que $\varnothing \subset A$, qualquer que seja o conjunto $A$. De fato, supor $\varnothing \not\subset A$, para algum $A$, significaria admitir o seguinte: existe um objeto $x$ tal que $x \in \varnothing$ e $x \notin A$. Como não pode ocorrer $x \in \varnothing$, entao deve se aceitar

que $\emptyset \subset A$. Convem notar ainda que $\emptyset \neq \{\emptyset\}$, pois o segundo desses conjuntos possui um elemento (o conjunto vazio), ao passo que o primeiro não possui nenhum.

## 2.5 Diagramas de Venn

Para ilustrar e visualizar relações entre conjuntos e operações com conjuntos, um instrumento bastante útil sao os chamados *diagramas de Venn*. A idéia é a seguinte: primeiro traça se um retângulo de dimensões arbitrarias para representar o conjunto de todos os elementos considerados. Depois, para representar cada subconjunto próprio do universo com que se esteja lidando, traça se um círculo no interior do retângulo. Por exemplo, a relação $A \subset B$ entre dois subconjuntos de $U$ é representada pelo diagrama a seguir.

## 2.6 Interseção e união

A *interseção* de dois conjuntos, $A$ e $B$, é o conjunto indicado por $A \cap B$ e definido pela propriedade "$x \in A$ e $x \in B$". Portanto:

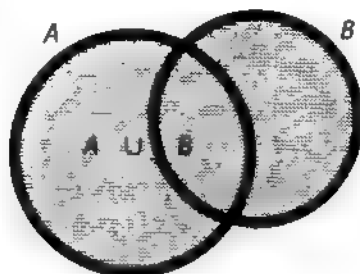
$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}$$

A operação que consiste em associar a cada dois conjuntos, dados numa certa ordem, sua interseção, goza das seguintes propriedades:

- $A \cap (B \cap C) = (A \cap B) \cap C$ (associatividade)
- $A \cap B = B \cap A$ (comutatividade)
- Se $A \subset B$, então $A \cap B = A$.
- $A \cap \emptyset = \emptyset$

Provemos a terceira dessas propriedades. Para tanto, consideremos inicialmente um elemento $x \in A \cap B$; então $x \in A$ e $x \in B$ (definição de interseção), o que garante que $A \cap B \subset A$. Seja, agora, $x \in A$; como $A \subset B$, então $x \in B$; logo, $x \in A \cap B$ e, portanto, $A \subset A \cap B$. As duas inclusões demonstradas garantem que, efetivamente, $A \cap B = A$ sempre que $A \subset B$.

A *união* de dois conjuntos, $A$ e $B$, é o conjunto indicado por $A \cup B$ e definido pela propriedade "$x \in A$ ou $x \in B$". Portanto:

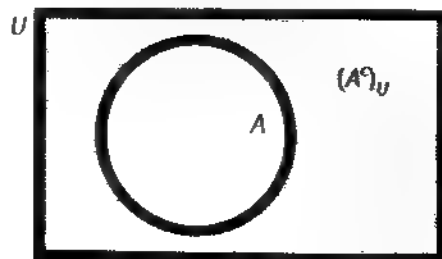
$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

Convém notar que o "ou" usado na definição não dá idéia de exclusividade: um elemento da união pode pertencer a ambos os conjuntos se a interseção não for vazia.

A operação que consiste em associar a cada dois conjuntos, dados numa certa ordem, sua união, cumpre as seguintes propriedades:

- $A \cup (B \cup C) = (A \cup B) \cup C$
- $A \cup B = B \cup A$
- Se $A \subset B$, então $A \cup B = B$.
- $A \cup \varnothing = A$

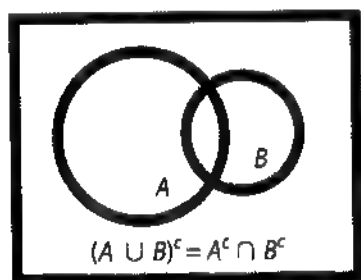
## 2.7 Complementar

Dados um conjunto $U$ e um subconjunto $A \subset U$, chama-se *complementar* de $A$ em relação a $U$ e denota-se por $(A^c)_U$ a parte de $U$ formada pelos elementos de $U$ que não pertencem a $A$. Ou seja:

$$(A^c)_U = \{x \in U \mid x \notin A\}$$

O conjunto $U$, cuja fixação é pressuposta na definição de complementar, é chamado *universo do discurso* ou *conjunto universo*. No desenvolvimento da matemática, trabalha-se, em cada situação, com um conjunto universo específico. Por exemplo, numa primeira abordagem do cálculo, o universo é o conjunto dos números reais e, na mesma situação, na teoria dos números (aritmética teórica), o universo é o conjunto dos números inteiros. Quando não houver dúvidas sobre qual o universo em que se está trabalhando, para simplificar a notação indicaremos o complementar de uma parte $A$ desse universo apenas por $A^c$.

Da definição de complementar decorrem as propriedades que seguem para um dado conjunto $U$ (universo) e para partes quaisquer, $A$ e $B$, de $U$.

- $U^c = \varnothing$ e $\varnothing^c = U$
- $(A^c)^c = A$
- $A \cap A^c = \varnothing$ e $A \cup A^c = U$
- $(A \cap B)^c = A^c \cup B^c$ e $(A \cup B)^c = A^c \cap B^c$

As duas últimas propriedades são conhecidas como *leis de De Morgan* ou *leis de dualidade*. A título de exercício, demonstremos que $(A \cup B)^c = A^c \cap B^c$. Seja $x$ um elemento de $U$. Se $x \in (A \cup B)^c$, então $x \notin A \cup B$ e, portanto, $x \notin A$ e $x \notin B$. Logo, $x \in A^c$ e $x \in B^c$, ou seja, $x \in A^c \cap B^c$, e fica provado que $(A \cup B)^c \subset A^c \cap B^c$. Agora, se $x \in A^c \cap B^c$, então $x \notin A$ e $x \notin B$ e, portanto, $x \notin A \cup B$ (se pertencesse a esse conjunto teria de pertencer a $A$ ou a $B$). De onde, $x \in (A \cup B)^c$, o que prova a inclusão contrária.

## Exercícios

1. Consideremos os seguintes subconjuntos de $\mathbb{R}$ (aqui considerado como conjunto universo): $A = \{x \in \mathbb{R} \mid x^2 < 4\}$, $B = \{x \in \mathbb{R} \mid x^2 - x \neq 2\}$, $C = \{1/2, 1/3, 1/4, \ldots\}$ e $D = \{x \in \mathbb{R} \mid 2 < x < 1\}$. Classifique cada relação seguinte como verdadeira ou falsa e justifique.

   a) $A^c \subset B$

   b) $A \cap B = D$

   c) $C \subset B^c$

   d) $B \cup A \supset C$

   e) $C \cap D \neq \varnothing$

**2.** Construa um exemplo envolvendo dois conjuntos, $B$ e $C$, para os quais se verifiquem as seguintes relações: $\varnothing \in C, B \in C, B \subset C$.

**3.** a) Descubra conjuntos, $A, B$ e $C$, tais que $B \neq C$ e $A \cup B = A \cup C$.
b) Com um exemplo, mostre que pode ocorrer o seguinte: $B \neq C$ e $A \cap B = A \cap C$

**4.** Se $A, B$ e $C$ são conjuntos tais que $A \cup B \quad A \cup C$ e $A \cap B \quad A \cap C$, prove que $B \quad C$.

**Resolução**

Seja $x \in B$. Então $x \in A \cup B = A \cup C$. Temos, aqui, duas possibilidades. $x \in A$ ou $x \in C$. Mas, se $x \in A$, então $x \in A \cap B = A \cap C$ e, portanto, $x \in C$. Assim, todo elemento de $B$ é também elemento de $C$. De maneira análoga, prova-se que todo elemento de $C$ é elemento de $B$. De onde, $B = C$. ■

**5.** Sejam $A$ e $B$ conjuntos tais que $A \cup B = A \cap B$. Prove que $A = B$.

**6.** Se $A$ e $B$ são conjuntos arbitrários, demonstre as seguintes propriedades (conhecidas como *leis de absorção*):

a) $A \cap (A \cup B) = A$
b) $A \cup (A \cap B) = A$

**7.** Dado um conjunto $A$, chama-se *conjunto das partes* de $A$ e indica-se por $\mathcal{P}(A)$ o conjunto de todos os subconjuntos de $A$. Por exemplo, se $A = \{1, 2\}$, então $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

a) Determine $\mathcal{P}(A)$ quando $A = \{\varnothing, 1, \{1\}\}$.
b) Prove que, se um conjunto $A$ tem $n$ elementos, então $\mathcal{P}(A)$ tem $2^n$ elementos.
c) Se o número de subconjuntos binários (formados de dois elementos) de um conjunto dado é 15, quantos subconjuntos tem esse conjunto?

**Resolução**

b) Como nos ensina a análise combinatória, o número de subconjuntos de $A$ com um elemento é $\binom{n}{1}$, o número de subconjuntos com dois elementos é $\binom{n}{2}$, etc. Como $\binom{n}{0} = 1$ e $\binom{n}{n} = 1$ podem ser usados para contar o conjunto vazio e o próprio $A$, então o total de subconjuntos de $A$ é $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}$. Mas essa soma, como nos ensina também a combinatória, é $2^n$. ■

**8.** Para indicar o número de elementos de um conjunto finito $X$, adotemos a notação $n(X)$. Mostre então que, se $A$ e $B$ são conjuntos finitos, verifica-se a importante relação: $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

**Resolução**

De fato, se indicarmos por $A'$ e $B'$, respectivamente, as partes de $A$ e $B$ formadas pelos elementos que não estão em $A \cap B$, então $n(A \cup B) = n(A') + n(A \cap B) + n(B')$. Mas $n(A') = n(A) - n(A \cap B)$ e $n(B') = n(B) - n(A \cap B)$. Substituindo estas duas últimas igualdades na anterior, obtemos a igualdade proposta. ■

**9.** Numa pesquisa a respeito da assinatura das revistas $A$ e $B$, foram entrevistadas 500 pessoas. Verificou-se que 20 delas assinavam a revista $A$, 14 a revista $B$ e 4 as duas revistas. Quantas das pessoas entrevistadas não assinavam nenhuma das revistas?

**10.** Se $A$, $B$ e $C$ são conjuntos finitos, mostre que:

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

**11.** Define-se a *diferença* entre dois conjuntos, $A$ e $B$, da seguinte maneira: $A - B = \{x \mid x \in A \text{ e } x \notin B\}$. Ache a diferença $A - B$ nos seguintes casos:

a) $A = \mathbb{Q}$ e $B = \mathbb{R}$
b) $A = \mathbb{R}$ e $B = \mathbb{Q}$
c) $A = \{x \in \mathbb{R} \mid 2 < x < 5\}$ e $B = \{x \in \mathbb{R} \mid x \geqslant 2\}$
d) $A = \{\frac{n}{n+1} \mid n = 1, 2, 3, ...\}$ e $B = \{\frac{2n}{2n+1} \mid n = 1, 2, 3, ...\}$
e) $A = \{x \in \mathbb{R} \mid 1 < x < 3\}$ e $B = \{x \in \mathbb{R} \mid x^2 - 3x - 4 > 0\}$

**12.** Sejam $A$ e $B$ conjuntos finitos tais que $n(A \cup B) = 40$, $n(A \cap B) = 10$ e $n(A - B) = 26$. Determine $n(B - A)$.

**13.** Denomina-se *diferença simétrica* entre dois conjuntos $A$ e $B$ e denota-se por $A \Delta B$ o seguinte conjunto: $A \Delta B = (A - B) \cup (B - A)$. Isso posto:

a) ache a diferença simétrica entre os pares de conjuntos do exercício 11;
b) mostre que, qualquer que seja o conjunto $A$, valem $A \Delta \varnothing = A$ e $A \Delta A = \varnothing$;
c) mostre que, para quaisquer conjuntos $A$ e $B$, vale $A \Delta B = B \Delta A$.

**14.** Sejam $A$ e $B$ subconjuntos de um conjunto $U$. Prove as seguintes propriedades:

a) Se $A \cap B = \varnothing$ e $A \cup B = U$, então $B = A^c$ e $A = B^c$.
b) Se $A \cap B = \varnothing$, então $B \subset A^c$ e $A \subset B^c$.
c) $B \subset A$ se, e somente se, $A^c \subset B^c$.

**15.** Prove as seguintes propriedades, envolvendo o conceito de diferença de conjuntos:

a) $(A \quad B) \cap (A \quad C) - A - (B \cup C)$

b) $(A - C) \cap (B - C) = (A \cap B) - C$

c) $(A \cup B) - B = A$ se, e somente se, $A \cap B = \emptyset$.

**Resolução**

b) Se $x \in (A - C) \cap (B - C)$, então $x \in A, x \notin C, x \in B$ e $x \notin C$. Daí $x \in A \cap B$ e, $x \notin C$ e, portanto, $x \in (A \cap B) - C$. Isso prova que $(A - C) \cap (B - C) \subset (A \cap B) - C$. Para provar a inclusão contrária, tomemos $x \in (A \cap B) - C$. Então, $x \in (A \cap B)$ e $x \notin C$. Daí $x \in A, x \in B$ e $x \notin C$ e, portanto, $x \in (A - C)$ e $x \in (B - C)$, ou seja, $x \in (A - B) \cap (A - C)$, como queríamos provar. ■

**16.** Encontre um exemplo para mostrar que pode ocorrer a desigualdade seguinte:

$$A \cup (B - C) \neq (A \cup B) - (A \cup C)$$

# I-2 SOBRE DEMONSTRAÇÕES

## 3. NOTA HISTÓRICA

A lógica, como ciência, foi criada por Aristóteles (384-322 a.C.). Mas, embora Aristóteles considerasse sua criação uma ciência independente da matemática e anterior a esta, as bases para a estruturação e sistematização da lógica empreendidas por ele já haviam sido lançadas antes pelos matemáticos gregos, ao criarem e desenvolverem o método dedutivo. De fato, esse método pressupõe, antes de tudo, leis corretas para o raciocínio, e isso se insere nos domínios da lógica. Entre essas leis, há que se destacar a *lei da não contradição*, que estatui que uma proposição não pode ser verdadeira e falsa ao mesmo tempo, e a *lei do terceiro excluído*, que estatui que uma proposição só pode ser verdadeira ou falsa, ambas introduzidas por Aristóteles.

A lógica de Aristóteles, cujas fórmulas (por exemplo, silogismos) se expressavam em palavras da linguagem comum, sujeitas a regras sintáticas comuns, reinou soberanamente até o século XIX — quando foi criada a lógica matemática —, a despeito do significativo papel desempenhado pela lógica escolástica da Idade Média.

Mas há que registrar, no século XVII, o trabalho desenvolvido por G. W. Leibniz (1646-1716) no sentido de criar uma álgebra simbólica formal para a lógica. A motivação para Leibniz foi a forte impressão que lhe causava o poder enorme da álgebra simbólica em campos diversos, e o objetivo de sua álgebra da lógica seria o de conduzir o raciocínio mecanicamente e sem esforços demasiados em todos os campos do conhecimento. Mas Leibniz deixou apenas escritos fragmentados sobre o assunto, escritos que, ademais, só se tornaram conhecidos em 1901.

Entre os matemáticos que contribuíram para a criação da lógica matemática no se-

culo XIX, aquele cuja obra teve peso e repercussão maiores foi G. Boole (1815-1864), graças sobretudo a *The laws of thought* ("As Leis do Pensamento"), de 1854. Uma ligeira idéia da obra de Boole pode ser dada por este fato ele usava letras minúsculas, $x$ $y$, $z$, ..., para indicar partes de um conjunto tomado como universo e representado pelo símbolo 1. Se $x$, $y$ representavam duas dessas partes, ele denotava o que hoje chamamos de *interseção* e *união* dessas partes respectivamente por $xy$ e $x + y$. O complementar de uma parte $x$ era indicado por $1 - x$. Na verdade, as uniões consideradas por Boole pressupunham partes disjuntas; a generalização, para o conceito atual, é devida a W. S. Jevons (1835-1882). Assim, sendo evidente que $xy = yx$, $x + y = y + x$, $xy = yx$, $(xy)z = x(yz)$, essas leis foram tomadas como axiomas em sua álgebra. Mas a nova álgebra apresenta diferenças fundamentais em relação à clássica: haja vista as leis $x^2 = x$ e $x + x = x$, para qualquer parte $x$ do universo.

Como exemplo do uso da álgebra de Boole, vejamos como se poderia colocar em símbolos a lei do terceiro excluído. Suponhamos que 1 indique o conjunto de todos os seres humanos vivos e $x$ o conjunto dos brasileiros vivos. Então, $1 - x$ indica o conjunto dos seres humanos vivos que não são brasileiros, e a equação $x + (1 - x) = 1$ expressa a idéia de que todo ser humano vivo ou é brasileiro ou não é brasileiro.

Não passou despercebida a Boole a correspondência entre a álgebra dos conjuntos e a das proposições. Se $p$ indica uma proposição, a equação $p = 0$ indica que $p$ é falsa, e a equação $p = 1$, que $p$ é verdadeira. Nesse contexto, dadas duas proposições, $p$ e $q$, ele indicava por $pq$ e $p + q$, respectivamente, a conjunção e a disjunção das duas. Mas Boole não se alongou muito nessa questão.

Tão importante e inovadora foi a obra científica de Boole, que o grande matemático e filósofo galês B. Russel (1872-1970) via nele o verdadeiro descobridor da matemática pura. Mas talvez nada ateste mais fielmente a importância dessa obra do que as muitas pesquisas que nela se inspiraram e que levariam a uma axiomatização da álgebra do pensamento no século XX.

## 4. DEMONSTRAÇÕES

### 4.1 Proposições e funções proposicionais

A matemática é uma ciência dedutiva. Isso significa, entre outras coisas, que a validade de um resultado matemático exige uma demonstração. Não é fácil definir o que é uma demonstração matemática. Basicamente, é uma sucessão articulada de raciocínios lógicos que permite mostrar que um resultado proposto é conseqüência de princípios previamente fixados e de proposições já estabelecidas. Nesse processo, é preciso lidar e operar constantemente com *proposições* (sentenças declarativas às quais se pode atribuir um *valor lógico* — verdadeiro ou falso, exclusivamente) e *funções proposicionais* (sentenças declarativas envolvendo variáveis).

Consideremos as sentenças "2 é um número primo", "$\sqrt{2}$ é um número racional" e "$x$ é um número real maior que 1". Como se vê, sao sentenças declarativas. Mas, embora se possa dizer que a primeira é verdadeira e a segunda falsa, nenhum valor lógico se pode atribuir à terceira, já que ela envolve uma variável em $\mathbb{R}$. As duas primeiras sao, pois, *proposições*, ao passo que a terceira é uma *função proposicional* (na variável $x$).

As variáveis de uma função proposicional sempre representam elementos de um conjunto previamente fixado — seu *domínio de validade* ou *universo*. As funções proposicionais na variável $x$ são indicadas em geral por $p(x), q(x), \ldots$ Toda função proposicional pode ser transformada numa proposição, bastando para isso substituir a variável por um elemento do universo. Se $a$ é um elemento do universo de $p(x)$, a proposição obtida com a substituição da variável por $a$ é indicada por $p(a)$. Por exemplo, se $p(x)$ é a função proposicional "$x^2 \geqslant 4$" no universo dos números racionais, então $p(3)$ é "$3^2 \geqslant 4$" (verdadeira) e $p(-1)$ é "$(-1)^2 \geqslant 4$" (falsa). Assim, uma maneira de transformar uma função proposicional em proposição é substituir a variavel (ou variáveis) por um elemento (ou elementos) arbitrário(s) do universo.

Outra maneira de transformar uma funçao proposicional em proposição consiste em quantificar a variável (ou variáveis), o que pode ser feito de duas maneiras: através do *quantificador existencial* "existe um pelo menos" ou do *quantificador universal* "qualquer que seja" (ou "qualquer" ou "todo"). No cálculo proposicional usam-se os símbolos $\exists$ e $\forall$ para indicar os quantificadores existencial e universal, respectivamente.

Por exemplo, a função proposicional "$x > 1$", em que $x$ é uma variável em $\mathbb{R}$, pode ser quantificada das maneiras que seguem.

"Existe um número real maior que 1" (verdadeira).

ou

"Todo número real é maior que 1" (falsa).

Se $p(x)$ é uma função proposicional cujo conjunto universo é $U$, então os elementos de $U$ que tornam verdadeira $p(x)$ constituem o que se chama *conjunto verdade* da proposição dada. Por exemplo, o conjunto verdade de "$x$ é um quadrado perfeito", em que $x$ é uma variável em $\mathbb{N}$, é $\{0, 1, 4, 9, \ldots\}$.

## 4.2 Conectivos

Na linguagem matemática, a *negação* de proposições ou funções proposicionais e a combinação de proposições ou funções proposicionais através dos conectivos "e" (conjunção), "ou" (disjunção), "se... então..." (condicional) e "se, e somente se" (bicondicional) são operações que têm interesse fundamental.

A respeito dos conectivos, convém esclarecer o seguinte.

• O *ou* usado na matemática não tem sentido exclusivo. Assim, numa proposição

disjuntiva, "$p$ ou $q$", ambas as proposições ($p$ e $q$) podem ser verdadeiras (ou falsas). Por exemplo, em "2 é primo ou 2 é par", ambas são verdadeiras.

• As proposições do tipo "se $p$ então $q$" serão entendidas aqui como " [$p$ e ( $q$)]". Assim, por exemplo, é o mesmo dizer que "Se uma pessoa e paulista, então essa pessoa é brasileira" ou "*Não* pode ocorrer de uma pessoa *ser paulista e não ser brasileira*". É o mesmo dizer também que "Se $x^2$ é um número par, então $x$ é um numero par" ou "*Nao* pode acontecer de $x^2$ *ser um número par* e $x$ *não ser um numero par*".

• Uma proposição do tipo "$p$ se, e somente se, $q$" será entendida como "se $p$, então $q$, e se $q$, então $p$".

No que segue, indicaremos por $\sim p$ a negação de uma proposição $p$.

Por exemplo, se $p$ indica a proposição "2 é primo" e $q$ a proposição "2 é par", então:

• "$\sim p$" (negação de $p$) é "2 não é primo";

• "$\sim q$" (negação de $q$) é "2 não é par" ou "2 é ímpar" (pois só há duas alternativas para um inteiro: par ou ímpar);

• "$p$ e $q$" é "2 é primo e 2 é par";

• "$p$ ou $q$" é "2 é primo ou 2 é par";

• "se $p$, então $q$" é "se 2 é primo, então 2 é par";

• "$p$ se, e somente se, $q$" é "2 é primo se, e somente se, 2 é par".

Nesse contexto, é importante saber determinar o valor lógico das proposições obtidas através da negação ou dos conectivos, em função do valor lógico das proposições dadas.

• Uma proposição "$\sim p$" é verdadeira se $p$ é falsa, e vice-versa.

• As proposições do tipo "$p$ e $q$" só são verdadeiras quando $p$ e $q$ são verdadeiras.

• As do tipo "$p$ ou $q$" só são falsas quando $p$ e $q$ são falsas.

• Para o estudo do valor lógico das condicionais "se $p$, então $q$" é melhor considerá-las na forma "$\sim$[$p$ e ($\sim q$)]". No caso em que $p$ e $q$ são verdadeiras, "$p$ e ($\sim q$)" é falsa (pois $\sim q$ é falsa) e, então, a negação dessa última, ou seja "se $p$, então $q$" é verdadeira; segue então que, quando $p$ e $q$ são verdadeiras, "se $p$, então $q$" é verdadeira. Aplicando-se esse raciocínio para os demais casos, conclui-se que uma proposição do tipo "se $p$, então $q$" só é falsa no caso em que $p$ é verdadeira e $q$ é falsa.

Como exemplo, consideremos as proposições "O menor número primo positivo é 2", que indicaremos por $p$, e "O menor número irracional positivo é $\sqrt{2}$", que indicaremos por $q$. Obviamente a primeira e verdadeira, e a segunda, falsa. Entao:

• "$\sim p$" e falsa;

• " $q$" é verdadeira;

• "$p$ e $q$" e falsa;

• "$p$ ou $q$" e verdadeira;

- "se $p$, então $q$" é falsa;
- "se $q$, então $p$" é verdadeira;
- "$p$ se, e somente se, $q$" é falsa (por quê?).

### 4.3 Implicação e equivalência

Se $p$ e $q$ são proposições tais que a condicional "se $p$, então $q$" é verdadeira, diz-se que $p$ *implica* ou *acarreta* $q$. Para indicar que $p$ implica $q$, usa-se a notação "$p \Rightarrow q$". Por exemplo:

$$1 > 2 \Rightarrow 4 \text{ é primo}$$

uma vez que a proposição "se $1 > 2$, então 4 é primo" é verdadeira (pois "$1 > 2$" é falsa). Por outro lado, não procederia escrever

$$2 > 1 \Rightarrow 4 \text{ é primo}$$

já que a primeira dessas proposições é verdadeira e a segunda falsa (único caso em que uma proposição do tipo "se... então..." é falsa, como vimos).

Sejam $p(x)$ e $q(x)$ funções proposicionais com o mesmo universo $U$. Se para todo $a \in U$ tal que $p(a)$ é verdadeira e a proposição $q(a)$ também for verdadeira, então se diz que $p(x)$ *acarreta* (ou *implica*) $q(x)$. A notação é a mesma: $p(x) \Rightarrow q(x)$. Por exemplo, se $U = \mathbb{R}$, então:

$$x > 2 \Rightarrow x^2 > 4$$

uma vez que todos os valores de $x$ que tornam verdadeira a primeira função proposicional também tornam verdadeira a segunda. Mas não procederia escrever

$$x^2 > 4 \text{ acarreta } x > 2$$

visto que há números reais que tornam verdadeira a primeira proposição e falsa a segunda (todos os números reais menores que $-2$).

Vale observar que, se no exemplo anterior o universo fosse o conjunto dos números reais positivos, então:

$$x^2 > 4 \Rightarrow x > 2$$

Uma importante propriedade de que goza a relação $\Rightarrow$ é a transitividade. Ou seja, se $p \Rightarrow q$ e $q \Rightarrow r$, então $p \Rightarrow r$. De fato, a proposição "se $p$, então $r$" só não seria verdadeira no caso de $p$ ser verdadeira e $r$ falsa. Mas, como "se $p$, então $q$" é verdadeira, então $q$ teria de ser verdadeira, e como "se $q$, então $r$" é verdadeira, então $q$ teria de ser falsa. Impossível, pois isso contraria o princípio da não-contradição. Então "se $p$, então $r$" é verdadeira e, portanto, $p \Rightarrow r$.

Duas proposições, $p$ e $q$, dizem-se logicamente *equivalentes* se $p \Rightarrow q$ e $q \Rightarrow p$. Notação: $p \Leftrightarrow q$. A definição de funções proposicionais equivalentes é análoga. Por exemplo:

$$x^2 - 4 = 0 \Leftrightarrow x = 2 \text{ ou } x = -2$$

De fato, os números reais que tornam verdadeira a primeira proposição (2 e  2) também tornam verdadeira a segunda, e vice-versa.

Consideremos uma implicação $p \Rightarrow q$ (poderia ser também uma implicação envolvendo funções proposicionais). Outra maneira de ler essa relação é:

"*p* é uma condição suficiente para *q*".

A explicação para isso é que a veracidade de *p* basta (é suficiente) para garantir a veracidade de *q*, uma vez que estamos supondo "se *p*, então *q*" verdadeira. Outra maneira ainda é:

"*q* é uma condição necessária para *p*".

A explicação, no caso, é que é necessária a veracidade de *q* para que se possa ter a veracidade de *p*.

Consideremos, por exemplo, a implicação "$x = 2 \Rightarrow x^2 = 4$", em que $x$ é uma variável em $\mathbb{R}$. Essa relação poderia, portanto, ser formulada de uma das seguintes maneiras: "$x$ ser igual a 2 é suficiente para que $x^2$ seja igual a 4" ou "$x^2 = 4$ é condição necessária para $x = 2$".

Isso justifica por que uma equivalência $p \Leftrightarrow q$ é comumente expressa nos seguintes termos:

"*q* é uma condição necessária e suficiente para *p*"

ou

"*p* é uma condição necessária e suficiente para *q*".

Por exemplo, a equivalência "$x$ é par $\Leftrightarrow x^2$ é par", em que $x$ representa um número inteiro, poderia ser formulada da seguinte maneira: "uma condição necessária e suficiente para que $x^2$ seja par é que $x$ seja par".

## 4.4 Recíproca de uma proposição ou função proposicional

A proposição "se *q*, então *p*" é chamada *recíproca* de "se *p*, então *q*". (Para funções proposicionais a definição é análoga.) É fácil ver que a recíproca de uma proposição verdadeira pode não ser verdadeira, e vice-versa. Ou seja, se *p* e *q* são proposições tais que "$p \Rightarrow q$" pode não valer a implicação contrária. O mesmo acontece com as funções proposicionais. Por exemplo, a recíproca de "Se $X$ é um quadrado, então $X$ é um losango" é "Se $X$ é um losango, então $X$ é um quadrado". Obviamente a primeira é verdadeira, mas a segunda não (nem todo losango é quadrado). Também pode acontecer de uma proposição e sua recíproca serem ambas verdadeiras ou falsas. Por exemplo, "Se $x^2$ é ímpar, então $x$ é ímpar" e sua recíproca "Se $x$ é ímpar, então $x^2$ é ímpar" são ambas verdadeiras.

## 4.5 Demonstração indireta — negação de funções proposicionais

Nos raciocínios matemáticos muitas vezes é preciso negar uma proposição. Isso acontece, especialmente, nas *demonstrações indiretas* ou *demonstrações por redução ao absurdo* de teoremas. Um teorema é basicamente uma proposição que, para ser admitida, precisa ser demonstrada. O enunciado de um teorema sempre explicita algumas *hipóteses* e pressupõe toda a teoria pertinente que o precede. O resultado a ser provado é a *tese*. Se a negação da tese levar a alguma contradição com as hipóteses ou com outros pressupostos da teoria, o teorema estará provado. Uma explicação formal rigorosa para esse fato requer um desenvolvimento do assunto fora dos objetivos deste texto e, por isso, nos ateremos a um exemplo.

Suponhamos que se deseja provar que "Se $m^2$ é ímpar, então $m$ também é ímpar" ($m$ número inteiro). Negando a tese, suponhamos que $m$ fosse par, ou seja, que pudesse ser escrito na forma $m = 2t$, em que $t$ é inteiro. Então $m^2 = 4t^2 = 2 \cdot (2t^2)$ também seria par, contra a hipótese. De onde, $m$ necessariamente é ímpar.

A seguir relacionaremos os procedimentos para as negações habitualmente necessárias na argumentação matemática.

• Se $p(x)$ indica uma função proposicional, a negação de "$(\forall x)(p(x))$" é "$(\exists x)(\sim p(x))$".

Por exemplo, a negação de "Qualquer que seja o número real $x$, $x^2$ é positivo" é "Existe um número real $x$ tal que $x^2$ é estritamente negativo". (Lembremos que, por nossa convenção, positivos são os números $\geq 0$ e estritamente negativos os números $< 0$).

• Se $p(x)$ indica uma função proposicional, a negação de "$(\exists x)(p(x))$" é "$(\forall x)(\sim p(x))$".

Por exemplo, a negação de "Existe um número real $x$ tal que $x^2$ 4 0" é "Qualquer que seja o número real $x$, vale $x^2 - 4 \neq 0$"

• Se $p$ e $q$ indicam proposições (ou funções proposicionais), a negação de "$p$ e $q$" é "$(\sim p)$ ou $(\sim q)$".

Por exemplo, a negação de "2 é par e 2 é primo" (ou "2 é par e primo", como seria mais comum dizer) é "2 não é par ou 2 não é primo".

• Se $p$ e $q$ indicam proposições (ou funções proposicionais), a negação de "$p$ ou $q$" é "$(\sim p)$ e $(\sim q)$".

Por exemplo, a negação de "Qualquer que seja o número real $x$, $x < 0$ ou $x \geq 0$" é "Existe um número real $x$ tal que $x \geq 0$ e $x < 0$".

• A negação da negação de uma proposição (ou função proposicional) $p$ é $p$.

Por exemplo, a negação de "3 não é ímpar" é "3 é ímpar".

• Se $p$ e $q$ indicam proposições (ou funções proposicionais), então a negação de "se $p$, então $q$" é "$p$ e $(\sim q)$".

A explicação para isso vem do fato de que "Se $p$, então $q$" tem formalmente o

mesmo sentido de "$\sim[p \text{ e } (\sim q)]$" e de que, se $s$ é uma proposição, então $\sim[\sim(s)]$ é $s$, como vimos anteriormente.

Como exemplo, consideremos a proposição "Se um número é racional, então também é um número real", que tem o mesmo sentido de "Todo número racional é real". Sua negação é "Existe um número que é racional e não é real"

## 4.6 Demonstração de existência

Na matemática são comuns os teoremas de existência. Nesse caso, a demonstração muitas vezes é feita simplesmente exibindo-se um objeto que cumpre a(s) condição(ões) desejada(s). Como exemplo, mostremos que dados dois números racionais, $a$ e $b$, com $a < b$, então existe um número irracional $\alpha$ tal que $a < \alpha < b$. De fato, o número

$$\alpha = a + \frac{b - a}{\sqrt{2}} \tag{1}$$

cumpre as condições desejadas. Observemos primeiro que, pela própria maneira como foi definido, o número $\alpha$ é maior que $a$ e menor que $b$. Por outro lado, de (1) segue que:

$$\sqrt{2} = \frac{b - a}{\alpha - a}$$

Assim, supondo que $\alpha$ fosse racional, então o segundo membro da última igualdade também seria um número racional e teríamos o seguinte absurdo: $\sqrt{2}$ racional. Logo, $\alpha$ é irracional.

É claro que exibir um objeto que cumpre uma determinada condição, em geral não é fácil, pois isso pode depender bastante de *insight* e bagagem matemática. Mas persistência e traquejo ajudam muito.

## 4.7 Demonstração por contra-exemplo

Há situações, também, em que se tem de demonstrar que uma proposição ou propriedade é falsa. Nesse caso, basta evidentemente dar um contra-exemplo. A título de ilustração, consideremos a seguinte proposição, no conjunto dos números inteiros: "Se $a$ é um divisor de $b$ e de $c$, então $a$ é um divisor de $b + c$". Como é bem conhecido, trata-se de uma proposição verdadeira. Mostremos que sua recíproca não é verdadeira. Essa recíproca pode ser enunciada assim: "Se $a$ é um divisor de $b + c$, então $a$ é um divisor de $b$ e $c$". Para mostrar a falsidade dessa última proposição, basta um contra-exemplo. E isso é fácil: 5 é um divisor de $3 + 7$, mas não é divisor de nenhuma das parcelas dessa soma.

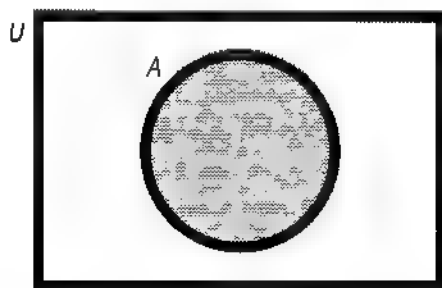
Para a descoberta de um contra-exemplo vale, com as devidas mudanças, a mesma observação feita ao final de **4.6**.

## 4.8 Contrapositiva de uma proposição ou função proposicional

Através do raciocínio por redução ao absurdo podemos mostrar que toda condicional "se *p*, então *q*" é logicamente equivalente à condicional "se ~*q*, então ~*p*", chamada *contrapositiva* da condicional dada. Mostremos, usando o raciocínio mencionado, que a primeira dessas condicionais implica a segunda. Para isso tomamos como hipótese "~ [*p* e ( *q*)]" (a maneira formal de escrever "se *p*, então *q*"). Observemos, porém, que a segunda condicional (no caso, a tese) pode ser substituída por " {(~*q*) e [~( *p*)]}", ou seja, por " [( *q*) e *p*]", cuja negação é "(~*q*) e *p*", proposição nitidamente contraditória com a hipótese. Essa contradição garante a validade da implicação considerada. Analogamente se demonstra a implicação contrária.

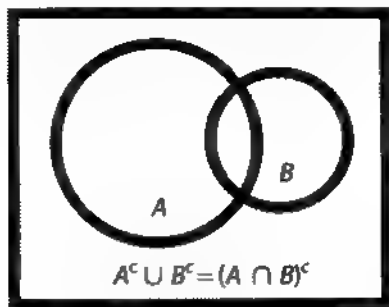
Como exemplo, consideremos a proposição "Se a soma de um número inteiro com seu quadrado é um número ímpar, então o número dado é ímpar". A contrapositiva dessa proposição é: "Se um número inteiro é par, então a soma desse número com seu quadrado é um número par". Pelo que vimos, demonstrar esse último resultado equivale a demonstrar o primeiro. E a vantagem, como em muitos casos, é que é mais fácil demonstrar essa última versão do teorema: basta representar um número par genericamente por $2t$ e fazer os cálculos algébricos indicados no enunciado: $(2t) + (2t)^2 = 2t + 4t^2 = 2(t + 2t^2)$, que é par.

## 4.9 Funções proposicionais e diagramas de Venn

Muitas vezes, no estudo de questões envolvendo funções proposicionais, é interessante representar ou imaginar o conjunto universo e os conjuntos verdade respectivos por meio de um diagrama de Venn, pois isso pode ajudar bastante o raciocínio. A figura a seguir mostra a representação do conjunto verdade *A* de uma proposição *p*(*x*) cujo conjunto universo é *U*.

Para utilizar esse expediente, é preciso, primeiro, estabelecer uma correspondência entre as funções proposicionais derivadas de uma ou duas funções proposicionais através da negação e dos conectivos e as partes correspondentes de *U*. Se *A* e *B* são, respectivamente, os conjuntos verdade de duas funções proposicionais *p*(*x*) e *q*(*x*), com o mesmo universo *U*, a tabela a seguir mostra essa correspondência.

| se $p(x)$, então $q(x)$ (no caso: $p(x) \Rightarrow q(x)$) | $A \subset B$ |
|---|---|
| $p(x)$ se, e somente se, $q(x)$ (no caso: $p(x) \Leftrightarrow q(x)$) | $A \quad B$ |
| $\sim[p(x)]$ | $A^c$ |
| $p(x)$ e $q(x)$ | $A \cap B$ |
| $p(x)$ ou $q(x)$ | $A \cup B$ |

Como exemplo, vejamos como se mostra a seguinte equivalência:

$$\sim[p(x) \text{ e } q(x)] \Leftrightarrow [\sim p(x) \text{ ou } \sim q(x)]$$

Para isso, indiquemos por $A$ e $B$, respectivamente, os conjuntos verdade de $p(x)$ e $q(x)$.

Então os pontos que tornam verdadeira "$\sim[p(x)$ e $q(x)]$" são os de $(A \cap B)^c = A^c \cup B^c$. Mas esse conjunto, por sua vez, é o conjunto verdade da função proposicional "$\sim p(x)$ ou $\sim q(x)$", o que completa nossa justificação.

## Exercícios

**17.** Qual é o valor lógico das seguintes proposições?

a) $2 + 5 = 1$ ou $3 > 1$.
b) 2 é primo e 2 é par.
c) Se $1 > 2$, então $1 = 2$.
d) Todo número primo é um número real.
e) Qualquer que seja o número real $x$, vale $x^2 > x$.
f) Existe um número real $x$ tal que $x^3 = -2$.
g) Para que um triângulo seja retângulo, é necessário e suficiente que o quadrado de um de seus lados seja igual à soma dos quadrados dos outros dois.
h) Se $f$ é uma função real de variável real, então $f$ é uma função par ou uma função ímpar.
i) Se $x$ é um número inteiro e $x^3$ é ímpar, então $x$ é ímpar.
j) Duas matrizes quadradas de mesma ordem são iguais se, e somente se, seus determinantes são iguais.

**18.** Considere que numa universidade se tenha a seguinte situação: há pesquisadores que não são professores e professores que não são pesquisadores; mas alguns pesquisadores são professores. Isso posto, quais das seguintes afirmações relativas a essa universidade são verdadeiras?

a) Existem professores que são pesquisadores.

b) Se $P$ indica o conjunto dos professores e $Q$ o conjunto dos pesquisadores, então $P \cap Q \neq \varnothing$.

c) Todo pesquisador é professor.

d) O conjunto dos professores não está contido no conjunto dos pesquisadores.

e) Existem pesquisadores que não são professores.

f) O conjunto dos pesquisadores está contido no conjunto dos professores.

**19.** Escreva na forma "se... então...":

a) Qualquer lado de um triângulo é menor que a soma dos outros dois lados.

b) Todo número primo diferente de 2 é ímpar.

c) Para um número real $x$ tal que $-2 < x < 2$, vale $x^2 < 4$

d) Duas retas quaisquer, paralelas entre si e não paralelas ao eixo das ordenadas, têm o mesmo coeficiente angular.

e) Sempre que uma função real de variável real é diferenciável num ponto, ela é contínua nesse ponto.

f) Um determinante é nulo quando uma de suas filas é formada de zeros.

**20.** Sejam $p$, $q$ e $r$ proposições, as duas primeiras verdadeiras e a terceira falsa. Indique o valor lógico de:

a) $p$ e $(\sim q)$;

b) $(\sim r)$ ou $(\sim p)$;

c) se ($p$ e $r$), então $q$;

d) $p$ se, e somente se, $r$.

**21.** Negue as seguintes proposições:

a) Se $x \in \mathbb{R}$ e $x > 2$, então $x^2 \geqslant 4$.

b) Nenhum triângulo retângulo é eqüilátero.

c) Qualquer que seja o número real $x$, existe um número inteiro $n$ tal que $n > x$.

d) Existe um número complexo $z$ tal que $z^5 = -2$.

e) Todo retângulo é um paralelogramo.

f) Se dois planos são paralelos, então toda reta de um deles é paralela ao outro plano.

**22.** Quantifique as funções proposicionais que seguem de modo a torná-las verdadeiras (para todas o universo é conjunto dos números reais)

a) $x^2 - 5x + 6 = 0$
b) $x^2 - 16 = (x - 4)(x + 4)$
c) $\text{sen}^2 x + \cos^2 x = 1$
d) $\text{sen}^2 x - \text{sen}\, x = 0$
e) $x^2 - 3x + 3 > 1$
f) $x^2 > 2x^3$

**23.** Se uma função proposicional envolve *n* variáveis, então é preciso quantificá-la *n* vezes a fim de que ela se torne uma proposição. Quanto a isso, é importante observar que os quantificadores existencial e universal nem sempre comutam entre si, como se pode verificar pelas proposições que seguem, a primeira verdadeira e a segunda falsa (em ambas o domínio da variável é $\mathbb{R}$): "Qualquer que seja $x$, existe $y$ tal que $x + y = 1$" e "Existe $x$ tal que, qualquer que seja $y$, $x + y = 1$".

Isso posto, quantifique as seguintes funções proposicionais de modo a torná-las verdadeiras (em todas, o universo das duas variáveis é o conjunto dos números reais):

a) $y > x$
b) $(x + y)^2 = x^2 + 2xy + y^2$
c) $x^2 \quad y$
d) $\text{sen}\,(x + y) - \text{sen}\, x + \text{sen}\, y$
e) $x^2 + y^2 \geqslant 0$

**24.** Determine o valor lógico das proposições seguintes, nas quais $x$ e $y$ são variáveis em $\{1, 2, 3\}$:

a) Existe $x$ tal que, qualquer que seja $y$, $x < y^2 + 1$.
b) Para todo $x$ existe $y$ tal que $x^2 + y^2 = 4$.
c) Existem $x$ e $y$ tais que $x^2 + y^2 = x^3$.

**25.** Em quais das condicionais seguintes é correto dizer que a primeira proposição (função proposicional na variável real $x$) acarreta a segunda?

a) Se $2 = 0$, então 4 é um número primo.
b) Se $x^2 + x - 2 = 0$, então $x = -2$.
c) Se $x$ é um número real, então $x$ é um número complexo.
d) Se $x^2 - 4 < 0$, então $x < 2$.
e) Se $\text{tg}\, x > 1$, então $x > \pi/4$.

**26.** Para quais das bicondicionais seguintes seria correto dizer que a primeira proposiçao (função proposicional) é equivalente à segunda?

a) $2x - 5 \geqslant 5$ se, e somente se, $x > 5$.

b) $x^2 + 3x + 2 < 0$ se, e somente se, $-2 < x < -1$.

c) sen $x$ = sen $(2x)$ se, e somente se, $x = 0$.

d) Uma matriz quadrada $A$ é inversível se, e somente se, $\det(A) \neq 0$.

e) As retas $y = 2x$ e $y = mx + n$ são perpendiculares se, e somente se, $2m + 1 = 0$.

**27.** Enuncie as recíprocas e as contrapositivas das seguintes proposições:

a) Se dois números inteiros são ímpares, então a soma deles é um número par.

b) Se uma função real de variável real é contínua num ponto, então ela é diferenciável nesse ponto.

c) Se uma matriz quadrada é inversível, então seu determinante é diferente de zero.

d) Se o grau de um polinômio real é 2, então esse polinômio tem duas e apenas duas raízes complexas.

e) Se dois planos são perpendiculares, então toda reta de um deles é perpendicular ao outro.

**28.** Classifique como verdadeiras ou falsas as recíprocas e as contrapositivas das proposições do exercício 27.

**29.** Enuncie a contrapositiva da propriedade transitiva da relação "maior que" em $\mathbb{R}$, ou seja, da propriedade: "Se $a > b$ e $b > c$, então $a > c$".

**30.** Enuncie a contrapositiva da seguinte proposição: "Sejam $A$, $B$ e $C$ pontos distintos de um plano. Se esses pontos não são colineares, então $AB < BC + AC$".

**31.** Ache um contra-exemplo para cada uma das seguintes afirmações:

a) Para todo $x \in \mathbb{R}$, $x^2 - 1 > 60$.

b) Para todo $x \in \mathbb{R}$, $x^3 - 4x^2 < 20$.

c) Para todo $x \in \mathbb{R}$, $\cos x > \cos(x + 1)$.

d) Para todo $x \in \mathbb{R}^*_+$, vale $\log_{10} x > \log_{10} x^2$.

**32.** Justifique a propriedade seguinte de duas maneiras, a primeira através de sua contrapositiva e a segunda por redução ao absurdo: "Se $m$ é um inteiro tal que $m^3 + 2$ é ímpar, então $m$ é ímpar".

**33.** Prove, por meio de um contra-exemplo, que $n^2 + n + 41$ (em que $n$ é um inteiro estritamente positivo) nem sempre é um número primo.

CAPÍTULO II

# INTRODUÇÃO À ARITMÉTICA DOS NÚMEROS INTEIROS

## 1. INTRODUÇÃO

No conjunto dos números naturais, que, segundo o matemático Leopold Kronecker (1823-1891), foi criado por Deus (o resto foi criado pelo homem, complementava ele), a diferença entre $a$ e $b$ só está definida se $a \geqslant b$. Mas há questões envolvendo a idéia de subtração de números naturais em que o minuendo é menor que o subtraendo — por exemplo, gastar mais do que se tem. Para enfrentar essas questões, foi preciso ampliar o conjunto dos números naturais, com a adjunção de novos números, os *números negativos*, introduzidos a princípio para possibilitar uma resposta a uma subtração qualquer de dois elementos de $\mathbb{N}$. Esse passo gerou naturalmente a necessidade de estender as operações e a relação de ordem de $\mathbb{N}$ ao novo conjunto, formado pelos números naturais e os números negativos.

Historicamente os inteiros negativos não foram os primeiros números a surgir dos naturais — as frações positivas vieram antes. Nem foram introduzidos de maneira bem estruturada e com bom acabamento matemático. Muito pelo contrário. Simplesmente surgiram, e de maneira bastante informal, em decorrência de questões práticas. Inicialmente na China, provavelmente bem antes do século III a.C., e mais tarde na Índia, em torno do século VI d.C. Mas na Europa ocidental do século XVII ainda

havia matemáticos de alto gabarito que não aceitavam bem (ou nem sequer aceitavam) os números negativos.

A idéia intuitiva é que, por exemplo, todas as "diferenças" $0 - 1, 1 - 2, 2 - 3, 3 - 4, \ldots$ de alguma maneira são "equivalentes" e representam o mesmo "número", um novo número que veio a ser indicado com o tempo por $-1$. De maneira análoga se introduzem os números $-2, -3, \ldots$. É claro que, sob o ponto de vista do rigor, esse procedimento deixa a desejar (o que são essas "diferenças", afinal?), mas os primeiros matemáticos a usá-lo não estavam preocupados com isso e foram em frente.

Obtidos esses novos números, é preciso ainda incorporá-los consistentemente ao conjunto dos números naturais (por uma questão de uniformidade, os números $1, 2, 3, \ldots$ são representados respectivamente por $+1, +2, +3, \ldots$), o que exige:

(i) Estender para o novo conjunto numérico, ou seja, $\mathbb{Z} = \{\ldots -3, -2, -1, 0, +1, +2, +3, \ldots\}$, as operações adição e multiplicação de números naturais. Isso significa, por exemplo, dar uma definição de adição no novo conjunto que, quando aplicada ao subconjunto dos números naturais (parte do novo conjunto), leve aos mesmos resultados que a adição de números naturais. Por exemplo, como $2 + 3 = (3 - 1) + (4 - 1) = (3 + 4) - (1 + 1) = 7 - 2 = 5$, é razoável esperar que $(-2) + (-3) = (1 - 3) + (1 - 4) = (1 + 1) - (3 + 4) = 2 - 7 = -5$ (notar que $2 - 7$ é uma das "diferenças" que definem $-5$).

(ii) Estender para $\mathbb{Z}$ a idéia de "menor" e "maior" a partir das (e coerentemente com as) idéias correspondentes em $\mathbb{N}$. Feito isso, podemos por fim nos referir a $\mathbb{Z}$ como o *sistema* (ou *campo*) dos *números inteiros*.

Obviamente essas considerações visam apenas dar uma idéia despretensiosa da construção dos números inteiros. Esse desenvolvimento, que, quando feito com rigor e formalismo, é bastante trabalhoso e até tedioso, foge ao plano traçado para este trabalho e, por isso, não será feito aqui. Começaremos considerando toda essa construção já feita, bem como conhecidas as propriedades básicas das operações e da relação de ordem em $\mathbb{Z}$.

## 2. INDUÇÃO

### 2.1 Princípio do menor número inteiro

Seja $L$ um subconjunto não vazio de $\mathbb{Z}$. Dizemos que $L$ é *limitado inferiormente* se existe um número $a \in \mathbb{Z}$ tal que $a \leqslant x$, qualquer que seja o elemento $x \in L$. Ou seja, $a$ menor que ou igual a qualquer elemento de $L$. Todo elemento $a \in \mathbb{Z}$ que cumpre essa condição chama-se *limite inferior* de $L$. Obviamente, se um inteiro $a$ é limite inferior de $L$, então todo inteiro menor que $a$ também o é. Um limite inferior de $L$ que pertença a esse conjunto chama-se *mínimo* de $L$. Pode-se provar que um subconjunto não vazio de $\mathbb{Z}$ não pode possuir mais do que um mínimo.

*Exemplo 1.* O conjunto $L = \{-2, -1, 0, 1, 2, 3, \ldots\}$ é limitado inferiormente e seus limites inferiores são $-2, -3, -4, \ldots$. E $L$ tem mínimo: o número $-2$.

*Exemplo 2:* O conjunto $S = \{\ldots, -6, -4, -2, 0\}$ dos múltiplos negativos de 2 não é limitado inferiormente. Obviamente não há nenhum inteiro que seja menor que todo elemento de $S$.

O resultado a seguir é um teorema quando se desenvolve a teoria dos numeros inteiros sistematicamente a partir dos números naturais. A palavra *princípio* que figura em sua designação deriva de razões históricas.

**Princípio do menor número inteiro:** Se $L$ é um subconjunto de $\mathbb{Z}$, não vazio e limitado inferiormente, então $L$ possui mínimo.

Por exemplo, o conjunto dos números inteiros positivos é limitado inferiormente e seu mínimo é o número 0.

## 2.2 Indução

Usando o princípio do menor número inteiro podem-se deduzir duas proposições bastante úteis para provar a veracidade de funções proposicionais definidas numa parte de $\mathbb{Z}$ limitada inferiormente.

**Primeiro princípio de indução:** Seja $p(n)$ uma função proposicional cujo universo é o conjunto dos inteiros maiores que ou iguais a um inteiro dado $a$. Suponhamos que se consiga provar o seguinte:

(i) $p(a)$ é verdadeira.

(ii) Se $r \geqslant a$ e $p(r)$ é verdadeira, então $p(r + 1)$ também é verdadeira.

Então $p(n)$ é verdadeira para todo $n \geqslant a$.

*Demonstração:* Seja $L = \{x \in \mathbb{Z} \mid x \geqslant a \text{ e } p(x) \text{ é falsa}\}$. Se mostrarmos que $L = \varnothing$, o princípio estará justificado. Para isso vamos raciocinar por redução ao absurdo. Suponhamos $L \neq \varnothing$. Então, uma vez que $L$ é limitado inferiormente ($a$ é um limite inferior), $L$ possui mínimo $l_0$. Como $p(a)$ é verdadeira, é claro que $l_0 > a$ e, então, $l_0 - 1 \geqslant a$. Por outro lado, $p(l_0 - 1)$ é verdadeira, já que $l_0 - 1$ está fora de $L$. Então, levando em conta a hipótese (ii), $p((l_0 - 1) + 1) = p(l_0)$ é verdadeira. Mas isso é absurdo, pois $l_0$ está em $L$. #

Como imagem para ilustrar o primeiro princípio de indução, costuma se usar o efeito dominó. Suponhamos uma fileira infinita de pedrinhas de dominó. Se a primeira pedra tomba para a frente, e o fato de uma pedra tombar faz com que a da frente também tombe, então todas as pedrinhas tombarão.

*Exemplo 3:* Mostremos que $1^2 + 2^2 + \ldots + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}$, sempre que $n \geqslant 1$. (No caso, a função proposicional $p(n)$ é a igualdade do enunciado.)

Para $n = 1$, o primeiro membro dessa igualdade é $1^2 = 1$ e o segundo $\frac{1(1+1)(2 \cdot 1+1)}{6} = \frac{6}{6} = 1$. Portanto, a função proposicional é verdadeira para $n = 1$.

Suponhamos que seja verdadeira para algum $r \geqslant 1$, isto é, suponhamos que $1^2 + 2^2 + \ldots + r^2 = \frac{r(r+1)(2r+1)}{6}$ seja verdadeira.

Então, para $n = r + 1$, o primeiro membro da igualdade a ser provada é

$$1^2 + 2^2 + \ldots + r^2 + (r+1)^2 = \frac{r(r+1)(2r+1)}{6} + (r+1)^2 = \frac{r(r+1)(2r+1)^2 + 6(r+1)^2}{6} =$$

$$= \frac{(r+1)(2r^2+r+6r+6)}{6} = \frac{(r+1)(2r^2+7r+6)}{6}$$

ao passo que o segundo é

$$\frac{(r+1)(r+2)(2(r+1)+1)}{6} = \frac{(r+1)(r+2)(2r+3)}{6} = \frac{(r+1)(2r^2+7r+6)}{6}$$

e, portanto, a função proposicional também é verdadeira para $n = r + 1$. Isso prova que a igualdade efetivamente vale para todo inteiro $n \geqslant 1$.

**Segundo princípio de indução:** Seja $p(n)$ uma função proposicional cujo universo é o conjunto dos inteiros maiores que ou iguais a um inteiro dado $a$. Suponhamos que se consiga provar o seguinte:

(i) $p(a)$ é verdadeira.

(ii) Se $r > a$ e $p(k)$ é verdadeira e para todo $k$ tal que $a \leqslant k < r$, então $p(r)$ também é verdadeira.

Então $p(n)$ é verdadeira para todo $n \geqslant a$.

A demonstração desse princípio é análoga à do primeiro e não será feita aqui (ver exercício 2).

*Exemplo 4:* Provemos, usando o segundo princípio de indução, que $n^2 \geqslant 2n$ para todo inteiro $n \geqslant 2$.

Para $n = 2$ o primeiro membro da desigualdade vale $2^2 = 4$ e o segundo $2 \cdot 2 = 4$. Portanto, a função proposicional é verdadeira para $n = 2$.

Seja $r > 2$ e suponhamos que se tenha $k^2 \geqslant 2k$ para todo inteiro $k$ tal que $2 \leqslant k < r$.

Façamos $r - k = t$, do que segue $r = k + t$, em que $t > 0$. Daí

$$r^2 = (k+t)^2 = k^2 + 2kt + t^2 \geqslant 2k + 2kt + t^2 > 2k + 2kt$$

Mas, como $k \geqslant 2$ e $t > 0$, então $2k > 2$ e, portanto, $2kt > 2t$. De onde:

$$r^2 > 2k + 2t = 2(k+t) = 2r$$

**Exercícios**

1. Demonstre por indução:

a) $1 + 2 + ... + n = \dfrac{n(n+1)}{2} \quad (n \geqslant 1)$

b) $1 + 3 + 5 + ... + (2n - 1) = n^2 \quad (n \geqslant 1)$

c) $1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2 \quad (n \geqslant 1)$

d) $1 \cdot 2 + 2 \cdot 3 + ... + n \cdot (n+1) = \dfrac{n(n+1)(n+2)}{3} \quad (n \geqslant 1)$

e) $n^2 > n + 1 \quad (n \geqslant 2)$

2. Demonstre o segundo princípio de indução.

# 3. DIVISIBILIDADE EM $\mathbb{Z}$

## 3.1 Divisão exata

Diz-se que o número inteiro $a$ é *divisor* do número inteiro $b$ ou que o número $b$ é *divisível* por $a$ se é possível encontrar $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso, pode-se dizer também que $b$ é *múltiplo* de $a$. Para indicar que $a$ divide $b$, usaremos a notação $a \mid b$.

Por exemplo, $-2$ divide 6 porque $6 = (-2)(-3)$. Também se pode afirmar que 0 divide 0 uma vez que, para todo inteiro $c$, $0 = 0 \cdot c$.

Se $a \mid b$ e $a \neq 0$, o número inteiro $c$ tal que $b = ac$ será indicado por $b/a$ e chamado *quociente* de $b$ por $a$.

A relação entre elementos de $\mathbb{Z}$, definida por $x \mid y$, que acabamos de introduzir, goza das seguintes propriedades:

**(i)** $a \mid a$ (reflexividade)

De fato, $a = a \cdot 1$.

**(ii)** Se $a, b \geqslant 0$, $a \mid b$ e $b \mid a$, então $a = b$.

Por hipótese, $b = a \cdot c_1$ e $a = bc_2$. Se $a = 0 (b = 0)$, então $b = 0 (a = 0)$. Suponhamos, pois, $a, b > 0$. Como $a = ac_1c_2$, segue que $c_1c_2 = 1$. Mas $c_1$ e $c_2$ são positivos e, portanto, essa igualdade só é possível para $c_1 = c_2 = 1$. De onde $a = b$.

**(iii)** Se $a \mid b$ e $b \mid c$, então $a \mid c$. (transitividade)

**(iv)** Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, quaisquer que sejam os inteiros $x$ e $y$.

Por hipótese, $b = ad_1$ e $c = ad_2$. Daí, $bx = a(xd_1)$ e $cy = a(yd_2)$. Somando membro a membro essas igualdades, obtemos:

$$bx + cy = a(xd_1) + a(yd_2) = a(xd_1 + yd_2)$$

Então, devido à definição dada, $a \mid (bx + cy)$.

Dessa propriedade, segue em particular que:

- Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $a \mid (b - c)$.
- Se $a \mid b$, então $a \mid bx$, qualquer que seja o inteiro $x$

**(v)** Se $a \mid b$ e $c \mid d$, então $ac \mid bd$

Por hipótese, $b = ar$ e $d = cs$ para convenientes inteiros $r$ e $s$. Multiplicando-se membro a membro essas igualdades, obtém-se $bd = (ac)(rs)$. De onde $ac \mid bd$.

*Exemplo 5:* Vamos provar que $h(n) = 2^{2n} + 15n - 1$ é divisível por 9, qualquer que seja o inteiro $n \geqslant 1$. A demonstração será feita por indução sobre $n$.

Como $h(1) = 2^{2 \cdot 1} + 15 \cdot 1 - 1 = 18 = 2 \cdot 9$, então a afirmação é verdadeira para $n = 1$.

Seja $r \geqslant 1$ e suponhamos $h(r)$ divisível por 9. Então $h(r) = 2^{2r} + 15r - 1 = 9 \cdot q$ para algum inteiro $q$. Segue daí que $2^{2r} = 9q - 15r + 1$.

Logo, $h(r+1) = 2^{2(r+1)} + 15(r+1) - 1 = 2^{2r} \cdot 2^2 + 15r + 15 - 1 = 4 \cdot 2^{2r} + 15r + 14 =$
$= 4(9q - 15r + 1) + 15r + 14 = 9(4q) - 60r + 15r + 18 = 9(4q) - 9(5r) + 9 \cdot 2 = 9(4q - 5r + 2)$, o que mostra que $h(r + 1)$ é múltiplo de 9.

Pelo primeiro princípio de indução, a propriedade está demonstrada.

## 3.2 Algoritmo euclidiano

Evidentemente, há infinitos casos de pares de inteiros tais que nenhum dos dois é divisor do outro. Por exemplo, nem 2 é divisor de 3, nem vice-versa. O algoritmo euclidiano, de que trataremos aqui, estabelece uma "divisão com resto" e é a base da aritmética teórica (teoria dos numeros). Seu nome deriva do fato de Euclides o haver usado em seus *Elementos* (c. 300 a.C.) para determinar o máximo divisor comum de dois números positivos. Nesse ponto nada mudou de lá para cá, como veremos. Diga-se de passagem, porém, que Euclides só considerava números inteiros estritamente positivos. Nosso contexto, aqui, é mais amplo.

Seja $a$ um número inteiro estritamente positivo. Tomando-se algum inteiro $b$, há duas possibilidades:

(i) $b$ é múltiplo de $a$ e, portanto, $b = aq$ para um conveniente inteiro $q$.

(ii) $b$ está situado entre dois múltiplos consecutivos de $a$, isto é, existe um inteiro $q$ tal que $aq < b < a(q + 1)$. Daí, $0 < b - aq < a$. Então, fazendo $b - qa = r$, obtemos $b = aq + r$, em que $0 < r < a$.

Juntando as duas possibilidades, podemos garantir o seguinte: dados dois inteiros, $a$ e $b$, com $a > 0$, então sempre se pode encontrar dois inteiros $q$ e $r$ tais que:

$$b = aq + r, \text{ em que } 0 \leqslant r < a$$

Evidentemente, $r = 0$ corresponde ao caso em que $b$ é múltiplo de $a$.

Vamos imaginar, por outro lado, que se pudesse determinar outro par de inteiros, $q_1$ e $r_1$, tais que $b = aq_1 + r_1$, com $0 \leqslant r_1 < a$. Então, $aq + r = aq_1 + r_1$ e,

portanto, $a(q - q_1) = r_1 - r$. Suponhamos que $r \neq r_1$, digamos $r > r_1$. Daí, o segundo membro da última igualdade seria estritamente negativo e, como $a > 0$, então $q - q_1$ também seria estritamente negativo e, portanto, $q_1 - q > 0$, ou seja, $q_1 - q \geq 1$. Mas de $a(q - q_1) = r_1 - r$ segue que:

$$r = r_1 + a(q_1 - q)$$

Levando-se em conta que $a > 0$, $r_1 \geq 0$ e $q_1 - q \geq 1$, da última igualdade seguiria que $r \geqslant a$, o que é absurdo.

Da mesma forma, prova-se que a desigualdade $r_1 > r$ também é impossível. De onde $r = r_1$ e, consequentemente, $q = q_1$.

O resultado acima, conhecido como *algoritmo euclidiano* ou *algoritmo da divisão em* $\mathbb{Z}$, garante a possibilidade de uma "divisão aproximada em $\mathbb{Z}$". Um enunciado geral para ele é o seguinte: "Dados um inteiro $b$ qualquer e um inteiro estritamente positivo $a$, podem-se determinar dois inteiros, $q$ e $r$, tais que $b = aq + r$, com $0 \leqslant r < a$. Ademais, as condições impostas determinam os inteiros $q$ e $r$ univocamente". Os elementos envolvidos no algoritmo têm nomes especiais: $b$ é o *dividendo*, $a$ é o *divisor*, $q$ é o *quociente*, e $r$ o *resto* na divisão euclidiana de $b$ por $a$. #

Na divisão de um inteiro $n$ por 2 há duas possibilidades: o resto ser 0 ou 1. No primeiro caso, o número é divisível por 2 e é chamado *número par*. Conseqüentemente, os números pares se apresentam sob a forma $2t$, em que $t$ é um inteiro. Se o resto for 1, o número pode ser expresso por $n = 2t + 1$, para algum inteiro $t$, e é chamado *número ímpar*. No caso da divisão de um inteiro $n$ por 3, os restos possíveis são 0, 1 ou 2 e, portanto, $n = 3t$, $n = 3t + 1$ ou $n = 3t + 2$, exclusivamente. E assim por diante.

*Exemplo 6:* Vamos determinar, usando o raciocínio da demonstração, o quociente e o resto da divisão de 97 por 6. Os múltiplos estritamente positivos de 6 são:

6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, ...

O número 97 está entre $96 = 6 \cdot 16$ e $102 = 6 \cdot 17$. Isso já nos dá o quociente: 16. O resto, de acordo com o algoritmo, é $r = 97 - 6 \cdot 16 = 1$.

*Exemplo 7:* Na divisão euclidiana de $-345$ por $a > 0$, o resto é 12. Determinar os possíveis valores de $a$ (divisor) e do quociente.

Se $q$ indica o quociente, então $-345 = a \cdot q + 12$ $(12 < a)$. Daí, $-357 = aq$, em que $a > 12$. Isso só é possível para $a = 357$ e $q = -1$, $a = 17$ e $q = -21$, $a = 21$ e $q = -17$, $a = 51$ e $q = -7$, $a = 119$ e $q = -3$.

## 3.3 Sobre o nosso sistema de numeração

Como é bem conhecido, nosso sistema de numeração, o mesmo usado hoje praticamente em todo o mundo civilizado, é *decimal posicional*. *Decimal* significa, em resumo que, para escrever todos os números, bastam dez algarismos ou dígitos, que

cada dez unidades de uma dada espécie constituem uma unidade da espécie imediatamente superior, unidade essa que, para efeito de numeração, toma o lugar das dez que a formaram. Dez unidades simples constituem uma dezena, dez dezenas uma centena, e assim por diante. *Posicional* significa, entre outras coisas, que os números são escritos na forma de seqüências finitas dos dez algarismos, cuja grafia modernamente é 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, e que o valor de um algarismo na sequência depende de sua posição, conforme ilustra o exemplo que segue. Em 234, o valor de 4 é efetivamente 4 unidades, o de 3 é $3 \cdot 10 = 30$ e o de 2 é $2 \cdot 10^2 = 200$. Na verdade, $234 = 4 + 3 \cdot 10 + 2 \cdot 10^2$.

Obviamente, a adoção desse sistema pressupõe que se possa fazer com qualquer número positivo o mesmo que se fez com o número do exemplo. Aliás, o objetivo principal deste tópico é dar uma idéia do porquê disso. Na verdade, como poderemos observar, ainda que de passagem, é possível construir um sistema de numeração posicional tomando como base qualquer número natural $b \geqslant 2$.

No curso da história, os sistemas posicionais plenos representam o ponto alto de um longo desenvolvimento. Mas certamente há bem mais de quatro milênios, os babilônios já tinham introduzido um sistema de numeração posicional, embora incompleto. Na verdade esse povo, por razões difíceis de explicar, criou um sistema de numeração misto muito avançado para a época. Até o número 59 era *decimal aditivo*, com apenas um símbolo para a unidade e um para a dezena. A fim de formar o numeral desejado, esses símbolos eram "adicionados" convenientemente — por exemplo, o símbolo do 10 ao lado do símbolo do 1 formava o símbolo do 11. A partir do número 60 era sexagesimal (de base 60) posicional, mas incompleto, uma vez que não utilizava sessenta símbolos, mas tão somente os mesmos dois já referidos e, num período final, um símbolo para o zero (mas mesmo assim só no interior de um numeral, não no fim).

𒁹 = 1

𒌋 = 10

Por exemplo, o símbolo 𒌋𒁹 podia indicar o 11 ou $1 + 10 \cdot 60 = 601$, ou mesmo outros números, dependendo do contexto ou até da proximidade dos símbolos.

O primeiro sistema de numeração decimal posicional surgiu na China, por volta do século XV a.C. Ele tinha, porém, características diferentes do nosso e, mesmo tendo evoluído ao longo do tempo, só há registro do uso de um símbolo para o zero, um

pequeno círculo, no século XIII Essa pode ser uma das razões pelas quais comumente se atribuem aos hindus a paternidade de nosso sistema de numeração. De fato, o mais tardar no século IX os hindus já tinham desenvolvido um sistema de numeração posicional decimal completo, essencialmente igual ao nosso, pois o persa Muhamed al-Khowarizmi, um dos grandes sábios da cultura árabe, o descreveu numa obra que data aproximadamente do ano 825, atribuindo-o aos hindus. Embora al-Khowarizmi só tivesse explicitado os símbolos dos algarismos de 1 a 9, fez uso do zero em seu trabalho. Um pequeno círculo que figura numa inscrição hindu do ano 878 parece ter sido o primeiro sinal usado para o zero na história de nosso sistema de numeração. O fato de este ser chamado comumente de *indo-arábico* deriva de o povo árabe ser o responsável por sua disseminação no Ocidente, na esteira da expansão de seus domínios territoriais, depois de o haver assimilado na Índia, uma de suas primeiras conquistas.

Na verdade, o que dá sustentação matemática ao uso de um sistema de numeração posicional é um teorema que enunciaremos a seguir para a base 10, mas que pode ser estendido, como se perceberá, para qualquer base (naturalmente $\geq 2$). Diga-se de passagem, porém, que os hindus não tinham um conhecimento da teoria envolvendo o sistema de numeração que criaram e que, se deram esse grande passo no desenvolvimento da matemática, foi unicamente com base no empirismo e na engenhosidade de seus matemáticos.

"Qualquer que seja o número natural $N$, é possível encontrar uma única seqüência $a_0, a_1, ..., a_r$ de números naturais, com $0 \leq a_i \leq 9$ ($i = 1, 2, ..., r$), tal que

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_r \cdot 10^r"$$

Esse resultado é uma decorrência do algoritmo euclidiano, e vamos fazer um esboço de justificação supondo $N \geq 10$ (o caso $N < 10$ é imediato). De fato, aplicando esse algoritmo para o número $N$ como dividendo e 10 como divisor, obtemos:

$$N = 10 \cdot q + r, \text{ em que } 0 \leq r \leq 9 \quad (1)$$

Se $0 \leq q \leq 9$, justificação encerrada, pois a igualdade

$$N = r + q \cdot 10$$

está de acordo com o enunciado, uma vez que $0 \leq q, r \leq 9$.

Se $q > 9$, aplica-se novamente o algoritmo, agora com $q$ como dividendo e 10 como divisor.

$$q = 10 \cdot q_1 + r_1, \text{ em que } 0 \leq r_1 \leq 9$$

Desta última igualdade e de (1), segue que

$$N = 10(10q_1 + r_1) + r = r + r_1 \cdot 10 + q_1 \cdot 10^2.$$

Se $0 \leq q_1 \leq 9$, justificação encerrada, pois $0 \leq r, r_1, q_1 \leq 9$. Caso contrário, usa-se o algoritmo para $q_1$ e 10. Prosseguindo nesse raciocínio, chegamos a uma

expressão do tipo da que foi dada para $N$ no enunciado. A questão da unicidade, embora também essencial, não será focalizada aqui.

O fato de um número $N$ poder ser expresso, univocamente, por uma expressão polinomial

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$$

permite que se represente esse número pela sequência

$$a_r a_{r-1} \ldots a_2 a_1$$

naturalmente subentendida a base dez. Por exemplo, o número $N = 5 \cdot 10^3 + 3 \cdot 10^2 + 9$ (nove unidades, três centenas e cinco milhares) é representado por

$$5309$$

em que o 0 indica a ausência de dezenas.

## Exercícios

**3.** Sejam $m$ e $n$ inteiros ímpares. Prove que:

a) $4 \mid (2m - 2n)$
b) $8 \mid (m^2 - n^2)$
c) $8 \mid (m^2 + n^2 - 2)$

**4.** Mostre que entre dois números pares consecutivos um é divisível por 4.

**5.** Mostre que a diferença entre os quadrados de dois inteiros consecutivos é sempre um número ímpar. E a diferença entre os cubos de dois inteiros consecutivos?

**6.** Demonstre por indução que:

a) $7 \mid (2^{3n} - 1) \quad (n \geqslant 0)$
b) $8 \mid (3^{2n} + 7) \quad (n \geqslant 0)$
c) $11 \mid (2^{2n-1} \cdot 3^{n+2} + 1) \quad (n \geqslant 1)$
d) $7 \mid (3^{2n+1} + 2^{n+2}) \quad (n \geqslant 1)$
e) $17 \mid (3^{4n+2} + 2 \cdot 4^{3n+1}) \quad (n \geqslant 0)$

**7.** Prove que:

a) Um dos inteiros $a, a + 2, a + 4$ é divisível por 3.
b) Um dos inteiros $a, a + 1, a + 2, a + 3$ é divisível por 4.

**8.** Prove que o produto de dois números inteiros é ímpar se, e somente se, ambos os números são ímpares.

**9.** Prove que, quaisquer que sejam os inteiros $a$ e $b$, a expressão $a + b + a^2 + b^2$ representa um número par.

**10.** Na divisão euclidiana de 802 por $a$, o quociente é 14. Determine os valores possíveis de $a$ e do resto.

**11.** É possível encontrar dois inteiros múltiplos de 5 tais que o resto da divisão euclidiana de um pelo outro seja 13? Justifique a resposta.

**12.** Quantos numeros naturais entre 1 e 1 000 são divisíveis por 9? Justifique a resposta.

**13.** Seja $m$ um inteiro cujo resto da divisão por 6 é 5. Mostre que o resto da divisão de $m$ por 3 é 2.

**Resolução**

Por hipótese, $m = 6q + 5$. Seja $r$ o resto da divisão de $m$ por 3 (portanto $m = 3q' + r$). Então $r = 0$, 1 ou 2. Basta mostrar que as duas primeiras alternativas são impossíveis. De fato, se $r = 0$, teríamos $m = 6q + 5 = 3q'$. Daí, $3 \cdot (q' - 2q) = 5$, igualdade essa que teria como consequência o seguinte absurdo: $3 \mid 5$. Logo, o resto não pode ser 0. Analogamente se demonstra que não pode ser 1. Portanto, $r = 2$. ■

**14.** Se o resto na divisão euclidiana de um inteiro $m$ por 8 é 5, qual é o resto da divisão de $m$ por 4?

**15.** Se $m$ é um inteiro ímpar, mostre que o resto da divisão de $m^2$ por 4 é 1.

## 4. MÁXIMO DIVISOR COMUM

**4.1** Consideremos, a título de ilustração, os inteiros 4 e 6. Os divisores de 4 são os elementos do conjunto $D(4) = \{\pm 1, \pm 2, \pm 4\}$, e os de 6 os do conjunto $D(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Os divisores comuns são os elementos da interseção desses dois conjuntos:

$$D(4) \cap D(6) = \{\pm 1, \pm 2\}$$

O maior elemento dessa interseção, ou seja, o número 2, é o *máximo divisor comum* de 4 e 6.

Essa forma de introduzir o máximo divisor comum, embora muito interessante sob o ponto de vista didático, principalmente nos níveis elementares, não é a mais conveniente para os objetivos deste trabalho. Por isso, a definição que segue (equivalente e óbvio, à que foi esboçada acima em termos de conjuntos de divisores).

**Definição 1:** Sejam $a$ e $b$ dois números inteiros. Um elemento $d \in \mathbb{Z}$ se diz *máximo divisor comum* de $a$ e $b$ se cumpre as seguintes condições.

i) $d \geq 0$

ii) $d \mid a$ e $d \mid b$

(iii) Se $d'$ é um inteiro tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$ (ou seja, todo divisor comum a $a$ e $b$ também é divisor de $d$).

A definição de máximo divisor comum pode ser estendida de maneira natural para $n$ números inteiros $a_1, a_2, ..., a_n$ $(n > 2)$.

*Exemplo 8.* É fácil comprovar que, no caso em que $a = 4$ e $b = 6$, o numero 2 é o único inteiro que passa pelo crivo das condições da definição dada. No caso de (iii), por exemplo, os divisores comuns a 4 e 6 são $\pm 1$, $\pm 2$, todos divisores de 2.

Seguem algumas propriedades imediatas do conceito de máximo divisor comum.

• Se $d$ e $d_1$ são máximos divisores comuns de $a$ e $b$, então $d = d_1$.

De fato, devido à definição, $d \mid d_1$ e $d_1 \mid d$. Como se trata de números positivos, isso só é possível se $d = d_1$. Fica garantido, então, que um dado par de inteiros não pode ter mais de um máximo divisor comum.

• O número 0 é o máximo divisor comum de $a = 0$ e $b = 0$. É só lembrar da definição.

• Qualquer que seja $a \neq 0$, $|a|$ é o máximo divisor comum de $a$ e 0.

De fato. Primeiro, $|a|$ é positivo. Depois, $|a|$ divide 0, porque todo inteiro é divisor de 0, como já vimos, e $|a|$ divide $a$, pois $a = |a|(\pm 1)$. Finalmente, se $c$ divide $|a|$ e $c \mid 0$, então $c \mid a$, pois $a = |a|(\pm 1)$.

• Se $d$ é máximo divisor comum de $a$ e $b$, então $d$ também é máximo divisor comum de $-a$ e $b$, $a$ e $-b$ e $-a$ e $-b$. Basta lembrar que todo divisor de $x$ é divisor de $-x$, e vice-versa.

**4.2** Obviamente, a definição de máximo divisor comum de dois números inteiros não garante por si só sua existência. A intuição nos diz que isso é verdade, mas, a rigor, é preciso demonstrar que é, o que faremos a seguir. A demonstração que daremos se justifica principalmente porque garante a possibilidade de exprimir de maneira aritmética o máximo divisor comum de $a$ e $b$ como uma soma envolvendo esses elementos.

**Proposição 1:** Para quaisquer inteiros $a$ e $b$, existem inteiros $x_0$ e $y_0$ tais que $d = ax_0 + by_0$ é o máximo divisor comum de $a$ e $b$.

*Demonstração:* Levando em conta a última propriedade imediata relacionada acima, podemos nos ater ao caso em $a > 0$ e $b > 0$.

Consideremos o conjunto $L = \{ax + by \mid x, y \in \mathbb{Z}\}$. $L$ possui elementos estritamente positivos, por exemplo, $a + b$, obtido ao se fazer $x = y = 1$. Seja $d$ o menor entre todos os elementos estritamente positivos de $L$. Portanto, $d = ax_0 + by_0$, para convenientes elementos $x_0, y_0 \in \mathbb{Z}$. Mostremos que $d$ é o máximo divisor comum de $a$ e $b$

De fato:

(i) Obviamente $d \geq 0$.

(ii) Apliquemos o algoritmo euclidiano a $a$ e $d$, o que é possível, pois $d > 0$: $a = dq + r$ $(0 \leq r < d)$. Mas, como já vimos, $d = ax_0 + by_0$ e, então:

$$a = (ax_0 + by_0)q + r$$

Daí, por transposições algébricas convenientes,

$$r = a(1 - qx_0) + b(-qy_0)$$

o que mostra que $r$ é um elemento de $L$. Então, $r$ não pode ser estritamente positivo, pois é menor que $d$ (= mínimo de $L$). Logo, $r = 0$ e, portanto, $a = dq$. Ou seja: $d \mid a$.

De maneira análoga se demonstra que $d \mid b$.

(iii) Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$, uma vez que $d = ax_0 + by_0$. #

Nesta altura já mostramos que todo par de inteiros tem um máximo divisor comum e que este é único. A notação que usaremos para exprimir o máximo divisor comum $d$ de $a$ e $b$ é $d = \text{mdc}(a, b)$. Vale salientar ainda que esse máximo divisor comum pode ser expresso por uma igualdade envolvendo $a$ e $b$: $d = ax_0 + by_0$, em que $x_0$ e $y_0$ são convenientes inteiros, como vimos. Na verdade, sempre há uma infinidade de pares de inteiros $x, y \in \mathbb{Z}$ para os quais $d = ax + by$. Cada uma dessas relações será chamada de *identidade de Bezout* para $a$, $b$ e $d$.

**4.3** A proposição anterior tem muitas vantagens, mas a desvantagem de não ser construtiva. Entretanto, esse problema pode ser superado, e a chave para isso é o algoritmo euclidiano. O *método de divisões sucessivas* para a determinação do máximo divisor comum de dois inteiros, que explicaremos a seguir, é o mesmo usado por Euclides há mais de dois milênios e ainda ensinado no ensino básico. Para tanto, precisaremos de dois lemas fáceis de provar. Sem prejuízo da generalidade, podemos nos ater a números inteiros estritamente positivos.

**Lema 1:** Se $a \mid b$, então $\text{mdc}(a, b) = a$.

*Demonstração:* Primeiro $a$ é estritamente positivo por hipótese. Depois $a \mid a$ e $a \mid b$ (hipótese). E se $d' \mid a$ e $d' \mid b$, é claro que $d' \mid a$. #

**Lema 2:** Se $a = bq + r$, então $d = \text{mdc}(a, b)$ se, e somente se, $d = \text{mdc}(b, r)$.

*Demonstração:* Suponhamos $d = \text{mdc}(a, b)$ e provemos que $d = \text{mdc}(b, r)$. Primeiro, $d > 0$, por hipótese. Depois, como $d \mid a$ e $d \mid b$, então $d \mid b$ e $d \mid (a - bq)$. Ou seja $d \mid b$ e $d \mid r$. Por último, se $d' \mid b$ e $d' \mid r$, então $d' \mid b$ e $d' \mid (bq + r)$, ou seja, $d' \mid b$ e $d' \mid a$; mas, como $d = \text{mdc}(a, b)$, então $d' \mid d$. A demonstração da recíproca segue a mesma linha de raciocínio. #

**Método das divisões sucessivas:** O objetivo é encontrar o máximo divisor comum de dois inteiros, $a$ e $b$ (que podemos supor estritamente positivos), por meio de aplicações sucessivas do algoritmo euclidiano. Primeiro, aplica-se para $a$ e $b$, depois para $b$ e o primeiro resto parcial, e assim por diante. Ou seja:

$$a = bq_1 + r_1 \qquad (0 \leq r_1 < b)$$
$$b = r_1q_2 + r_2 \qquad (r_2 < r_1)$$
$$r_1 = r_2q_3 + r_3 \qquad (r_3 < r_2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

É claro que, se acontecer de $r_1$ ser nulo, então $b = \text{mdc}(a, b)$, devido ao lema 1, e o processo termina na primeira etapa. Se $r_1 \neq 0$, passa-se à segunda e raciocina-se da mesma maneira com relação a $r_2$. Se $r_2 = 0$, então $r_1 = \text{mdc}(b, r_1)$, devido ao lema 1; mas, devido ao lema 2, $\text{mdc}(b, r_1) = \text{mdc}(a, b)$, das duas conclusões obtidas, segue que $r_1 = \text{mdc}(a, b)$. E assim por diante.

Ocorre que, como $b > r_1 > r_2 > \ldots \geq 0$, então para algum índice $n$ teremos com certeza $r_{n+1} = 0$. De fato, se todos os elementos de $\{r_1, r_2, r_3, \ldots\}$ fossem não nulos, então esse conjunto, que é limitado inferiormente, não teria mínimo, o que é impossível. Assim, para o índice $n$ referido:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$
$$r_{n-1} = r_n \cdot q_{n+1}$$

Portanto, em virtude dos lemas demonstrados:

$$r_n = \text{mdc}(r_{n-1}, r_n) = \text{mdc}(r_{n-2}, r_{n-1}) = \ldots = \text{mdc}(b, r_1) = \text{mdc}(a, b)$$

*Exemplo 9:* Determinar, pelo processo das divisões sucessivas, mdc(41, 12). Devido ao papel especial que têm, sublinharemos o dividendo, o divisor e o resto em cada etapa do processo.

$$\underline{41} = \underline{12} \cdot 3 + \underline{5}$$
$$\underline{12} = \underline{5} \cdot 2 + \underline{2}$$
$$\underline{5} = \underline{2} \cdot 2 + \underline{1}$$
$$\underline{2} = \underline{1} \cdot 2 \qquad (2)$$

Portanto, mdc(41,12) = 1.

Usualmente, porém, procede-se da seguinte maneira:

| | 3 | 2 | 2 | 2 |
|---|---|---|---|---|
| 41 | 12 | 5 | 2 | **1** |
| 5 | 2 | 1 | 0 | |

*Exemplo 10:* O processo das divisões sucessivas também serve para determinar os inteiros $x_0$, $y_0$ tais que $ax_0 + by_0 = d$, em que $d = \text{mdc}(a, b)$. Vamos ilustrar o procedimento para $a = 41$ e $b = 12$. Para isso, aproveitaremos as divisões sucessivas já feitas em (2). Começaremos pela penúltima igualdade, aquela em que o máximo divisor comum figura como resto, pondo $\underline{1}$ em função de $\underline{5}$ e $\underline{2}$, por meio de transposições algébricas. Na igualdade obtida, substituímos 2 em função de 12

e $\underline{5}$ e continuamos com o processo até obter o maximo divisor comum, 1, em função de $4\underline{1}$ e $1\underline{2}$. Vejamos como:

$$\underline{1} = \underline{5} - 2 \cdot 2 = \underline{5} - (1\underline{2} - \underline{5} \cdot 2) \cdot 2 = 5 \cdot 5 + \underline{12} \cdot (-2) =$$
$$= (4\underline{1} - 1\underline{2} \cdot 3) \cdot 5 + 1\underline{2} \cdot (-2) = \underline{41} \cdot 5 + 1\underline{2} \cdot (-\underline{17})$$

Entao um par de valores para $x_0$ e $y_0$ tal que $41x_0 + 12y_0 = 1$ é $(5, -17)$

**4.4** Dois inteiros $a$ e $b$ dizem-se *primos entre si* se $mdc(a, b) = 1$. Por exemplo, os números 41 e 12 são primos entre si, uma vez que, como já vimos em **4.3**, $mdc(41, 12) = 1$.

**Proposição 2:** Para que os inteiros $a$ e $b$ sejam primos entre si, é necessário e suficiente que se possam encontrar $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$.

*Demonstração:* Se $a$ e $b$ são primos entre si, então a proposição 1 garante a existência do par de elementos $x_0$, $y_0$ conforme o enunciado.

Reciprocamente, suponhamos que se possam encontrar $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Então, qualquer divisor de $a$ e $b$ é também divisor de 1. Logo, os únicos divisores comuns aos elementos $a$ e $b$ são $+1$ e $-1$. De onde o máximo divisor comum de $a$ e $b$ é 1. #

*Exemplo 11:* Mostremos que dois números inteiros consecutivos são primos entre si. Sejam $n$ e $n + 1$ os números. Se $a \mid n$ e $a \mid n + 1$, então $a \mid [(n+1) - n]$, ou seja, $a \mid 1$. Logo, $a = \pm 1$, quer dizer, os únicos divisores comuns a $n$ e $n+1$ são 1 e $-1$. De onde $mdc(n, n+1) = 1$.

Outra maneira de chegar a essa conclusão é observar que vale a seguinte identidade de Bezout para os números considerados: $(n + 1) \cdot 1 + n(-1) = 1$.

**Corolário:** Se $a$ e $b$ são inteiros não simultaneamente nulos e se $d = mdc(a, b)$, então $mdc(a/d, b/d) = 1$.

*Demonstração:* É só trabalhar com uma identidade de Bezout para $a$ e $b$. Como $d = mdc(a, b)$, então existem inteiros $x_0$ e $y_0$ tais que $ax_0 + by_0 = d$. Daí (dividindo ambos os membros por $d$):

$$(a/d)x_0 + (b/d)y_0 = 1$$

Então, por causa da proposição, $a/d$ e $b/d$ são primos entre si. #

**Proposição 3:** Se $a$ e $b$ são inteiros primos entre si e $a \mid bc$, então $a \mid c$

*Demonstração.* Devido à proposição anterior, $ax_0 + by_0 = 1$, para convenientes inteiros $x_0$ e $y_0$. Multiplicando-se os dois membros dessa igualdade por $c$:

$$(ac)x_0 + (bc)y_0 = c$$

Como $a$ divide $a$, então $a$ divide $(ac)x_0$; e, como $a$ divide $bc$ (por hipótese), então divide $(bc)y_0$. Logo, $a$ divide a soma $(ac)x_0 + (bc)y_0$. Ou seja, $a$ divide $c$, como queríamos provar. #

**Proposição 4:** Sejam $a$ e $b$ inteiros primos entre si. Se $a \mid c$ e $b \mid c$, então $ab \mid c$.

*Demonstração:* Consideremos uma identidade de Bezout para $a$ e $b$:

$$ax_0 + by_0 = 1$$

Multiplicando-se ambos os membros dessa igualdade por $c$:

$$(ac)x_0 + (bc)y_0 = c$$

Como $a \mid a$ e $b \mid c$, então $ab \mid ac$ e, portanto, $ab \mid (ac)x_0$; de maneira análoga, demonstra-se que $ab \mid (bc)y_0$. Logo, $ab \mid [(ac)x_0 + (bc)y_0]$, ou seja, $ab \quad c$. #

## Exercícios

**16.** Encontre o máximo divisor dos pares de números que seguem e, para cada caso, dê uma identidade de Bezout.

a) 20 e 74 b) 68 e 120 c) 42 e $-96$

**17.** O máximo divisor comum de dois números é 48 e o maior deles é 384. Encontre o outro número.

**18.** O máximo divisor comum de dois números é 20. Para se chegar a esse resultado pelo processo das divisões sucessivas, os quocientes encontrados foram, pela ordem, 2, 1, 3 e 2. Encontre os dois números.

**19.** a) Prove que mdc(a, mdc($b$, $c$)) $-$ mdc($a$, $b$, $c$).

b) Use esse fato para encontrar o máximo divisor comum de 46, 64 e 124.

**Resolução**

a) Seja $d$ $-$ mdc($a$, $b$, $c$) e provemos que $d$ mdc($a$, mdc($b$, $c$)) (i) $d \geqslant 0$, pela definição de máximo divisor comum. (ii) Como $d \mid a$, $d \mid b$ e $d \mid c$, por hipótese, então $d \quad a$ e $d \mid$ mdc($b$, $c$), visto que todo divisor de $b$ e $c$ é divisor do máximo divisor comum desses números. (iii) Seja $d'$ um divisor de $a$ e de mdc($b$, $c$); então $d' \mid a$, $d' \mid b$ e $d' \mid c$ e, portanto, divide o maximo divisor comum desses números, ou seja, divide $d$.

b) Fica proposto. ■

**20.** Prove que mdc($n$, $2n + 1$) = 1, qualquer que seja o inteiro $n$.

**21.** Sejam $a$ e $b$ números inteiros tais que mdc($a$, $a+b$) = 1. Prove que mdc($a$, $b$) = 1. O recíproco desse resultado também é verdadeiro. Enuncie-o e demonstre-o. *Sugestão:* Para a primeira parte, tome um divisor de $c$ de $a$ e $b$ e mostre que ele também é divisor de $a$ e $a + b$.

**22.** Demonstre que, se $a \mid c$, $b \mid c$ e $\text{mdc}(a, b) = d$, então $ab \mid cd$.

*Sugestão:* Use a identidade de Bezout para $a$, $b$ e $d$.

**23.** Se $a$ e $b$ são inteiros primos entre si, demonstre que $\text{mdc}(2a + b, a + 2b) = 1$ ou 3.

## 5. NÚMEROS PRIMOS

**5.1** Um número inteiro $a \neq 0, \pm 1$ tem pelo menos quatro divisores: $\pm 1$ e $\pm a$. Esses são os *divisores triviais* de $a$. Alguns números diferentes de 0 e $\pm 1$ só têm os divisores triviais — são os chamados *números primos*. Por exemplo, o número 2 é primo, pois seus únicos divisores são $\pm 1$ e $\pm 2$. Um número inteiro diferente de 0 e $\pm 1$ e que tem divisores não triviais é chamado *número composto*. O 6, por exemplo, cujos divisores são $\pm 1, \pm 2, \pm 3$ e $\pm 6$.

**Definição 2:** Um número inteiro $p$ é chamado *número primo* se as seguintes condições se verificam:

(i) $p \neq 0$

(ii) $p \neq \pm 1$

(iii) Os únicos divisores de $p$ são $\pm 1, \pm p$.

Um número inteiro $a \neq 0, \pm 1$ é chamado *número composto* se tem outros divisores, além dos triviais.

**Lema 3** (lema de Euclides): Sejam $a, b, p \in \mathbb{Z}$. Se $p$ é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

*Demonstração:* Suponhamos que $p$ não seja um divisor de $a$. Logo, $-p$ também não é divisor de $a$. Como os divisores de $p$ são apenas $\pm 1$ e $\pm p$, então os divisores comuns a $p$ e $a$ são apenas $\pm 1$. Daí, $\text{mdc}(p, a) = 1$ e, portanto, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$px_0 + ay_0 = 1$$

Multiplicando-se ambos os membros dessa igualdade por $b$, obtém-se:

$$p(bx_0) + (ab)y_0 = b$$

Como $p \mid p$ e $p \mid ab$ (hipótese), então $p \mid [p(bx_0) + (ab)y_0]$, ou seja, $p \mid b$. Analogamente se mostra que, se $p$ não divide $b$, então divide $a$. #

Por indução, pode-se demonstrar sem dificuldades maiores que, se $p$ é primo e divide $a_1a_2...a_n$ $(n \geqslant 1)$, então $p$ divide um dos fatores $a_i$.

**Lema 4:** Seja $a \neq 0, \pm 1$ um inteiro. Então, o conjunto

$$L = \{x \in \mathbb{Z} \mid x > 1 \text{ e } x \text{ é divisor de } a\}$$

possui um mínimo e esse mínimo é um número primo.

*Demonstração:* O conjunto $L$ não é vazio, pois $a$ e $-a$ são divisores de $a$ e um desses números é necessariamente maior que 1. Então, pelo princípio do menor

número inteiro, $L$ possui mínimo, o qual será denotado por $p$. Se $p$ não fosse primo, então seria composto (já que é maior que 1), teria um divisor não trivial $q$ e, portanto, também $-q$ seria divisor de $p$. Resumindo: $p$ teria um divisor $q_1$ tal que $1 < q_1 < p$ ($q_1 = q$ ou $q_1 = -q$). Juntando as conclusões: $p \mid a$ e $q_1 \mid p$, do que segue que $q_1 \mid a$ e, portanto, $q_1 \in L$. Absurdo, já que $p$ é o mínimo de $S$ e $1 < q_1 < p$ #

**Proposição 5** (teorema fundamental da aritmética): Seja $a > 1$ um numero inteiro. Então é possível expressar $a$ como um produto $a = p_1p_2...p_r$, em que $r \geq 1$ e os inteiros $p_1, p_2, ..., p_r$ são números primos positivos. Além disso, se $a = q_1q_2...q_s$, em que $q_1, q_2, ..., q_s$ são também números primos positivos, então $s = r$ e cada $p_i$ é igual a um dos $q_j$.

*Demonstração:*

(i) Para demonstrar a possibilidade da decomposição, a rigor se deveria raciocinar por indução. Mas nossa explicação será meio informal. Devido ao lema 4, $a$ tem um divisor primo positivo $p_1$. Logo, $a = p_1q_1$, para um conveniente $q_1 \in \mathbb{Z}$. Como $a$ e $p_1$ são estritamente positivos, o mesmo acontece com $q_1$, que, ademais, é menor que $a$ (é um fator positivo de $a$). Se $q_1 = 1$, demonstração concluída: $a = p_1$ é primo positivo. Se $q_1 > 1$, repete-se o raciocínio com esse número: toma-se um divisor primo $p_2$ de $q_1$, o que é garantido pelo lema 4, e, portanto, $q_1 = p_2q_2$, para um conveniente inteiro positivo $q_2$ ($q_2 < q_1$). Nesta altura: $a = p_1p_2q_2$, em que $p_1$ e $p_2$ são primos e $q_2 \geqslant 1$. Agora repete-se o raciocínio com $q_2$, e assim por diante. Como $a > q_1 > q_2 > ... \geqslant 1$, em alguma etapa desse procedimento se terá $q_r = 1$ e, então, $a = p_1p_2...p_r$, como queríamos provar.

(ii) Também aqui não nos preocuparemos com o rigor formal. Suponhamos $p_1p_2...p_r = q_1q_2...q_s$, nas condições enunciadas. Então $p_1$, por exemplo, divide o segundo membro e, portanto, devido ao lema 3, divide um dos fatores. Digamos que $p_1 \mid q_1$. Como $q_1$ é primo e seu único divisor primo positivo é ele mesmo, então $p_1 = q_1$. Então, pode-se cancelar $p_1$ na igualdade da hipótese, obtendo-se $p_2p_3...p_r =$ $= q_2q_3...q_s$. Repete-se o raciocínio, o que permitirá cancelar um fator do primeiro membro com um igual a ele do segundo. E assim por diante. Como, evidentemente, não se pode ter uma situação do tipo $p_{s+1}\,p_{s+2}...p_r = 1$ (pois isso significaria que os números primos do primeiro membro seriam divisores de 1, o que é impossível), então $r = s$ e cada fator do primeiro membro é igual a um do segundo. #

Convém frisar que a demonstração da possibilidade da decomposição é construtiva, como se pôde observar. Mais: a idéia dessa demonstração é usada no algoritmo prático com o qual normalmente se aprende na escola a decomposição em fatores primos. De fato, suponhamos que se queira decompor em fatores primos o número 60. O algoritmo usado começa, como ocorre na demonstração, considerando-se o menor divisor primo de 60, que no caso é 2. Depois se considera, também

como na demonstração, o menor divisor primo do quociente, que no caso novamente é 2, e assim por diante. O algoritmo prático costuma ser ensinado da maneira que segue:

$$\begin{array}{r|l} 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

Portanto, $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$.

## 5.2 Sobre a decomposição em fatores primos

A proposição anterior, dada sua importância, merece alguns comentários e especificações. Na decomposição de um inteiro estritamente positivo $a$ em fatores primos positivos, conforme o teorema, pode ocorrer de um fator se repetir algumas vezes. Nesse caso podem-se reunir esses fatores repetidos numa só potência, mediante a notação exponencial. Supondo que os fatores primos distintos sejam $p_1 < p_2 < ... < p_m$ $(m \geq 1)$ e que eles apareçam respectivamente $\alpha_1, \alpha_2, ..., \alpha_m$ vezes $(\alpha_i \geq 1, i = 1, 2, ..., m)$, a decomposição poderá ser escrita assim:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$$

Essa decomposição, com os fatores primos em ordem crescente, será tratada como *decomposição canônica* de $a$ em fatores primos.

Mas muitas vezes lida-se numa mesma questão com dois ou mais inteiros estritamente positivos. Quando isso acontece, pode ser conveniente ampliar a idéia de decomposição canônica para que em todas figurem os mesmo fatores primos. Isso é sempre possível recorrendo-se ao uso do expoente nulo. Assim, se um fator primo aparece na primeira decomposição com expoente não nulo e não aparece explicitamente na segunda, nós o inserimos nesta com expoente igual a 0. Com essa convenção, supondo que os inteiros sejam $a$ e $b$, podemos escrevê-los assim:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} \quad \text{e} \quad a = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r} \quad (\alpha_i, \beta_i \geq 0) \qquad (3)$$

Por exemplo, os números 28 e 300 podem ser representados da seguinte forma:

$$28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7 \quad \text{e} \quad 300 = 2^2 \cdot 3 \cdot 5^2 \cdot 7^0$$

Através desse expediente pode-se construir o máximo divisor comum de dois elementos estritamente positivos (e, por conseqüência, de qualquer par de inteiros $\neq 0, \pm 1$). De fato, supondo-se que esses elementos sejam $a$ e $b$ e que sejam dados por (3), então o elemento

$$d = p_1^{\gamma_1} p_2^{\gamma_2} ... p_r^{\gamma_r}$$

em que $\gamma_i = \min\{\alpha_i, \beta_i\}$, é o máximo divisor comum de $a$ e $b$.

De fato, obviamente $d$ é positivo; além disso, como $\gamma_i \leq \alpha_i$ e $\gamma_i \leq \beta_i$, então $d \mid a$ e $d \mid b$; por último, se $d' \in \mathbb{Z}$ e $d' \mid a$ e $d' \mid b$, então

$$d' = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}$$

com $\gamma_i \leq \alpha_i$ e $\gamma_i \leq \beta_i$. Portanto, $\gamma_i \leq \min\{\alpha_i, \beta_i\}$. De onde $d' \mid d$.

Por exemplo, se $a = 28$ e $b = 300$, como

$$28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7 \quad \text{e} \quad 300 = 2^2 \cdot 3 \cdot 5^2 \cdot 7^0$$

então

$$\text{mdc}(28, 300) = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 4$$

*Exemplo 12:* Através da decomposição canônica

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

pode-se obter uma fórmula para o número de divisores de $a$. De fato, um número positivo é divisor de $a$ se, e somente se,

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$$

em que $0 \leq \beta_i \leq \alpha_i$ ($i = 0, 1, 2, \dots, m$). Como para cada expoente na decomposição de $b$ há $\alpha_i + 1$ possibilidades a fim de que $b$ divida $a$, então o número de divisores positivos de $a$ é

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$$

Por exemplo, o número de divisores positivos de $300 = 2^2 \cdot 3 \cdot 5^2$ é $3 \cdot 2 \cdot 3 = 18$.

## Exercícios

**24.** Decomponha em fatores primos 234, 456 e 780.

**25.** Ache o máximo divisor comum dos seguintes pares de números através da decomposição desses números em fatores primos:

a) 234 e 456
b) 456 e 780
c) 200 e 480

**26.** Determine todos os números primos que podem ser expressos na forma $n^2 - 1$.
*Sugestão:* Suponha $p = n^2 - 1$ um número primo e fatore o segundo membro dessa igualdade.

**27.** Se $n$ é um inteiro e $n^3 - 1$ é primo, prove que $n = 2$ ou $n = -1$.

**28.** Em 1742, o russo Christian Goldbach formulou a seguinte conjectura (conhecida como *conjectura de Goldbach*). "Todo inteiro par maior que 2 é igual à soma de

dois números primos positivos". Por exemplo: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, etc. Até hoje continua em aberto a questão de saber se essa proposição é falsa ou verdadeira.

Admitindo a conjectura de Goldbach, prove que todo inteiro maior que 5 é soma de três números primos. Por exemplo: $6 = 2 + 2 + 2$, $7 = 2 + 2 + 3$, $8 = 2 + 3 + 3$, etc.

*Sugestão:* Devido à conjectura, se $n \geqslant 3$, $2n - 2 = p + q$ ($p$ e $q$ primos). Portanto, $2n = p + q + 2$ (soma de três números primos).

**29.** Ache o menor número inteiro positivo $n$ para o qual a expressão $h(n) = n^2 + n + 17$ é um número composto.

**30.** Se $n^2 + 2$ é um número primo, prove que $n$ é múltiplo de 3 ou $n = 1$.

*Sugestão:* Há três possibilidades de expressar um número inteiro $n$: $n = 3q$, $n = 3q + 1$, $n = 3q + 2$, conforme o resto da divisão de $n$ por 3 seja 0, 1 ou 2. Mostre que as duas últimas são impossíveis, no caso.

**31.** Qual é o menor número inteiro positivo que tem15 divisores?

*Sugestão.* Se $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ é a decomposição do número procurado em fatores primos, então $15 = (\alpha_1 + 1)(\alpha_2 + 1)\dots(\alpha_m + 1)$. Observe que só há duas maneiras (salvo quanto à ordem) de decompor 15 em fatores inteiros positivos.

**32.** Demonstre que o conjunto dos números primos positivos é infinito

A primeira demonstração conhecida desse resultado, aliás a mesma que esboçaremos a seguir, foi dada por Euclides em seus *Elementos*

*Esboço da demonstração:* Suponha que esse conjunto fosse finito: digamos que seus elementos fossem $p_1, p_2, \dots, p_n$. Construa o número $p = p_1 p_2 \dots p_n + 1$. Esse número não é nenhum dos $p_i$ (por quê?). Logo, é composto (por quê?). Então é divisível por um dos $p_i$ ($1 \leqslant i \leqslant n$) (por quê?). Segue, então, que $p \mid 1$ (por quê?). Esse absurdo (por quê?) garante a infinitude do conjunto dos primos.

## 6. EQUAÇÕES DIOFANTINAS LINEARES

**6.1** Diofanto de Alexandria viveu provavelmente no século III d.C. De sua produção matemática conhecem-se apenas os fragmentos de uma obra que trata de números poligonais e a extremamente original e criativa *Arithmetica*, graças à qual ele é às vezes considerado o pai da álgebra. Da *Arithmetica* restam seis livros em grego e quatro em árabe, estes últimos descobertos recentemente (segundo o prefácio da obra, o número total de livros seria treze). Trata-se de uma coletânea de problemas, para resolução dos quais Diofanto usava, em vez de métodos gerais, engenhosos artifícios algébricos. Com isso a obra se distingue radicalmente da matemática grega clássica

(de Euclides, por exemplo), cujas raízes estavam fincadas na geometria e no método dedutivo.

Devido à *Arithmetica*, hoje são chamadas *equações diofantinas* todas as equações polinomiais (não importa o número de incógnitas) com coeficientes inteiros, sempre que seu estudo seja feito tomando como universo das variáveis o conjunto dos números inteiros. Isso não obstante Diofanto só ter trabalhado com alguns poucos casos particulares dessas equações e seu universo numérico ter sido o dos números racionais estritamente positivos.

Aqui só estudaremos as equações diofantinas lineares em duas incógnitas. Ou seja, equações do tipo

$$ax + by = c \tag{4}$$

em que $a$ e $b$ são inteiros não nulos. Uma solução de (4) é, nesse contexto, um par $(x_0, y_0)$ de inteiros tais que a sentença

$$ax_0 + by_0 = c$$

é verdadeira. Inicialmente deduziremos uma condição para que (4) tenha uma solução.

**Proposição 6:** Uma equação diofantina linear $ax + by = c$ tem solução se, e somente se, $d = \text{mdc}(a, b)$ é um divisor de $c$.

*Demonstração:*

($\rightarrow$) Se $(x_0, y_0)$ é uma solução, vale a igualdade

$$ax_0 + by_0 = c$$

Como $d \mid a$ e $d \mid b$, então $d \mid c$, devido à propriedade **(iv, 3.1)**.

($\leftarrow$) Como $d = \text{mdc}(a, b)$, então, devido à proposição 1, podem-se determinar $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = d$. Mas, por hipótese, $d \mid c$ e, portanto, $c = dq$ para algum inteiro $q$. De onde,

$$c = dq = (ax_0 + by_0)q = a(x_0q) + b(y_0q)$$

o que mostra que o par $(x_0q, y_0q)$ é solução da equação considerada. #

É importante observar que, se $(x_0, y_0)$ é uma solução de $ax + by = c$, com $a, b > 0$, então $(-x_0, y_0)$, $(x_0, -y_0)$ e $(-x_0, -y_0)$ são soluções respectivamente de $(-a)x + by = c$, $ax + (-b)y = c$ e $(-a)x + (-b)y = c$.

*Exemplo 13:* Encontrar uma solução da equação diofantina $26x + 31y = 2$. Como $\text{mdc}(26, 31) = 1$, então a equação tem solução. Usaremos o método das divisões sucessivas para exprimir o máximo divisor de 26 e 31 por meio de uma identidade de Bezout.

$$\underline{31} = 26 \cdot 1 + 5$$
$$\underline{26} = \underline{5} \cdot 5 + \underline{1}$$
$$5 = \underline{1} \cdot 5$$

Assim,

$$1 = \underline{26} - \underline{5} \cdot 5 = \underline{26} - (\underline{31} - \underline{26} \cdot 1) \cdot 5 = 26 \cdot 6 + \underline{31} \cdot (-5)$$

Então $(x_0, y_0) = (6, -5)$ e, portanto, o par $(2 \cdot 6, 2 \cdot (-5)) = (12, -10)$ é uma solução da equação dada.

Consequentemente $(-12, -10)$, $(12, 10)$ e $(-12, 10)$ são soluções, respectivamente, de $(-26)x + 31y = 2$, $26x - 31y = 2$ e $(-26)x + (-31y) = 2$.

**Proposição 7:** Se a equação diofantina $ax + by = c$ tem uma solução $(x_0, y_0)$, então tem infinitas soluções e o conjunto destas é

$$S = \{(x_0 + (b/d)t, y_0 - (a/d)t) \mid t \in \mathbb{Z}\}$$

em que $d = \text{mdc}(a, b)$.

*Demonstração:* Mostremos primeiro que todo par $(x_0 + (b/d)t, y_0 - (a/d)t)$ é solução da equação considerada. De fato,

$$a(x_0 + (b/d)t) + b(y_0 - (a/d)t) = ax_0 + by_0 + [(ab - ba)/d]t = ax_0 + by_0 = c$$

pois $(x_0, y_0)$ é solução, por hipótese.

De outra parte, seja $(x', y')$ uma solução genérica da equação. Então:

$$ax' + by' = c = ax_0 + by_0$$

Daí,

$$a(x' - x_0) = b(y_0 - y')$$

Mas, como $d$ é divisor de $a$ e de $b$, então $a = dr$ e $b = ds$, para convenientes inteiros $r$ e $s$, primos entre si. Logo,

$$dr(x' - x_0) = ds(y_0 - y')$$

e, portanto:

$$r(x' - x_0) = s(y_0 - y')$$

Essa igualdade mostra que $r$ divide $s(y_0 - y')$. Mas, como $r$ e $s$ são primos entre si, então $r$ divide $y_0 - y'$ (proposição 3). Logo:

$$y_0 - y' = rt$$

para algum $t \in \mathbb{Z}$. Levando-se em conta que $r = a/d$, então

$$y' = y_0 - (a/d)t$$

Observando-se agora que, em conseqüência,

$$r(x' - x_0) = s(y_0 - y') = srt$$

obtém-se:

$$x' = x_0 + (b/d)t \quad \#$$

É interessante e talvez surpreendente observar que o fato de uma equação diofantina $ax + by = c$ ter infinitas soluções (quando tem uma) significa, geometricamente, que a reta de equação $ax + by = c$ possui uma infinidade de pontos de coordenadas inteiras do plano cartesiano.

*Exemplo 14:* Determinar todas as soluções da equação diofantina $43x + 5y = 250$.

Como $\text{mdc}(43, 5) = 1$, que obviamente divide 250, a equação tem soluções. É importante lembrar que, se $(x_0, y_0)$ é uma solução de $43x + 5y = 1$, então $(250x_0, 250y_0)$ é solução da equação dada, como já vimos.

Mas já vimos também como achar uma solução de $43x + 5y = 1$ por divisões sucessivas. Da sucessão

$$\begin{aligned} \underline{43} &= \underline{5} \cdot 8 + \underline{3} \\ \underline{5} &= \underline{3} \cdot 1 + \underline{2} \\ \underline{3} &= \underline{2} \cdot 1 + \underline{1} \end{aligned}$$

segue que

$\underline{1} = \underline{3} - \underline{2} \cdot 1 = \underline{3} - (\underline{5} - \underline{3} \cdot 1) \cdot 1 = \underline{3} \cdot 2 + \underline{5} \cdot (-1) = (\underline{43} - \underline{5} \cdot 8) \cdot 2 + \underline{5} \cdot (-1) = \underline{43} \cdot 2 +$ $+ \underline{5} \cdot (-17)$ e, portanto, uma solução de $43x + 5y = 1$ é $(2, -17)$. Logo, uma solução de $43x + 5y = 250$ é $(500, -4\,250)$. De onde a solução geral da equação pode ser expressa por

$$(500 + 5t, -4250 - 43t)$$

em que $t$ é uma variável no conjunto dos inteiros.

Conforme observação ao fim da demonstração da proposição 7, a reta de equação $43x + 5y = 250$ possui uma infinidade de pontos de coordenadas inteiras do plano cartesiano.

### Exercícios

**33.** Resolva as seguintes equações diofantinas lineares:

a) $3x + 4y = 20$

b) $5x - 2y = 2$

c) $18x - 20y = -8$

d) $24x + 138y = 18$

**34.** Decomponha o número 100 em duas parcelas positivas tais que uma é múltiplo de 7 e a outra de 11. (Problema do matemático L. Euler [1707-1783].)

**35.** Ache todos os números inteiros estritamente positivos com a seguinte propriedade: dão resto 6 quando divididos por 11 e resto 3 quando divididos por 7.

**36.** O valor da entrada de um cinema é R$ 8,00 e da meia entrada R$ 5,00. Qual é o menor número de pessoas que pode assistir a uma sessão de maneira que a bilheteria seja de R$ 500,00? (Em tempo: a capacidade desse cinema é suficiente para esse número de pessoas.)

**37.** Ao entrar num bosque, alguns viajantes avistam 37 montes de maçã. Após serem retiradas 17 frutas, o restante foi dividido igualmente entre 79 pessoas. Qual a parte de cada pessoa? (Problema de Mahaviracarya, matemático hindu.)

## 7. CONGRUÊNCIAS

**7.1** O conceito de congruência, bem como a notação através da qual essa noção se tornou um dos instrumentos mais poderosos da teoria dos números, foi introduzido por Karl Friedrich Gauss (1777 1855), em sua obra *Disquisitiones arithmeticae* (1801)

Para dar uma idéia da noção de congruência, consideremos a seguinte questão, talvez ingênua mas ilustrativa: se hoje é sexta-feira, que dia da semana será daqui a 1520 dias?

Para organizar o raciocínio, indiquemos por 0 o dia de hoje (sexta-feira), por 1 o dia de amanhã (sábado), e assim por diante. A partir dessa escolha, pode-se construir o seguinte quadro:

| sexta | sábado | domingo | segunda | terça | quarta | quinta |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| ... | ... | ... | ... | ... | ... | ... |

Nossa questão agora se resume em saber em que coluna da tabela se encontra o numero 1520. Para isso basta observar que dois números da sequência 0, 1, 2, ... estão na mesma coluna se e somente se, sua diferença é divisível por 7. Suponhamos que o numero 1520 se encontre na coluna encabeçada pelo número $a$ ($0 \leq a \leq 6$). Então,

$$1520 \quad a \quad 7q$$

para algum inteiro positivo $q$. Daí.

$$1520 = 7q + a \quad (0 \leq a \leq 6)$$

Ora, pe a unicidade do resto na divisão euclidiana, segue dessa igualdade que $a$ é o resto da divisão de 1520 por 7. Observando que

```
1520 |_7___
12     217
 50
  1
```

conclui-se que esse resto é 1 e que, portanto, 1520 está na segunda coluna. Logo, daqui a 1520 dias será um sábado.

Questões como essa, envolvendo periodicidade, exigem uma aritmética diferente. O conceito de congruência, a ser dado a seguir, é a chave dessa aritmética.

**Definição 3:** Sejam $a$, $b$ números inteiros quaisquer e $m$ um inteiro estritamente positivo Diz se que $a$ é *côngruo* a $b$ módulo $m$ se $m$ , ($a$ · $b$), Isto é, se $a \quad b = mq$ para um conveniente inteiro $q$ Para indicar que $a$ é côngruo a $b$, modulo $m$, usa se a notação

$$a \quad b \ (\text{mod } m)$$

A relação assim definida sobre o conjunto $\mathbb{Z}$ chama-se congruência módulo $m$.

Por exemplo, na tabela construída na abertura deste tópico, dois elementos quaisquer de uma mesma coluna são côngruos módulo 7.

Para indicar que $a - b$ não é divisível por $m$, ou seja, que $a$ não é congruo a $b$ módulo $m$, escreve-se

$$a \not\equiv b \pmod{m}$$

Seguem as propriedades básicas da congruência de inteiros:

**C$_1$)** $a \equiv a \pmod{m}$ (*reflexividade*)

De fato, $a - a = 0$ é divisível por $m$.

**C$_2$)** Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$. (*simetria*)

Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$, ou seja, $a - b = mq$ para algum $q$. Daí $b - a = m(-q)$ e, portanto, $m \mid (b - a)$. De onde $b \equiv a \pmod{m}$.

**C$_3$)** Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$. (*transitividade*)

Por hipótese, $m \mid (b - a)$ e $m \mid (c - b)$. Logo, $m \mid [(b - a) + (c - b)]$, ou seja, $m \mid (c - a)$. Daí, $m \mid (a - c)$ e, portanto, $a \equiv c \pmod{m}$.

**C$_4$)** Se $a \equiv b \pmod{m}$ e $0 \leq b < m$, então $b$ é o resto da divisão euclidiana de $a$ por $m$. Reciprocamente, se $r$ é o resto da divisão de $a$ por $m$, então $a \equiv r \pmod{m}$.

De fato. Por hipótese, $a - b = mq$ para algum inteiro $q$. Daí $a = mq + b$ $(0 \leq b < m)$. A conclusão decorre da unicidade do quociente e do resto no algoritmo euclidiano.

A demonstração da recíproca é imediata.

**C$_5$)** $a \equiv b \pmod{m}$ se, e somente se, $a$ e $b$ dão o mesmo resto na divisão euclidiana por $m$.

$(\rightarrow)$ Por hipótese, $a - b = mq$, para algum inteiro $q$. Portanto:

$$a = b + mq$$

Sejam $q_1$ e $r$ o quociente e o resto da divisão euclidiana de $a$ por $m$:

$$a = mq_1 + r \quad (0 \leq r < m)$$

Das duas últimas igualdades segue que

$$b + mq = mq_1 + r$$

e, então:

$$b = m(q_1 - q) + r \quad (0 \leq r < m)$$

Portanto, r é o resto da divisão de $b$ por $m$.

$(\leftarrow)$ Por hipótese, $a$ e $b$ dão o mesmo resto na divisão euclidiana por $m$:

$$a = mq_1 + r \quad \text{e} \quad b = mq_2 + r \quad (0 \leq r < m)$$

Subtraindo-se membro a membro essas igualdades:

$$a - b = m(q_1 - q_2)$$

De onde, $a \equiv b \pmod{m}$.

Todo conjunto formado por um e um só elemento de cada classe de equiva-

lência módulo $m$ é chamado *sistema completo de restos módulo* m. Obviamente, como o representante mais natural da classe $\bar{r}$ é o elemento $r$, então o conjunto $\{0, 1, 2, ..., m - 1\}$ é o sistema completo de restos módulo $m$ mais natural. Mas nem sempre é o mais conveniente. São também sistemas completos de restos módulo $m$, às vezes mais convenientes:

- $\left\{0, \pm 1, \pm 2, ..., \pm \frac{m-1}{2}\right\}$, se $m$ é ímpar.

- $\left\{0, \pm 1, \pm 2, ..., \pm\left(\frac{m}{2} - 1\right), \frac{m}{2}\right\}$, se $m$ é par.

Para mostrar, por exemplo, que a congruência $x^2 + 1 \equiv 0 \pmod 8$ não tem solução, o uso deste último sistema facilita. De fato, como

$$x \equiv 0, \pm 1, \pm 2, \pm 3, 4 \pmod 8$$

então $x^2 \equiv 0, 1, 4, 9, 16 \pmod 8$. Mas $9 \equiv 1 \pmod 8$ e $16 \equiv 0 \pmod 8$. Portanto, $x^2 \equiv 0, 1, 4 \pmod 8$. De onde, $x^2 + 1 \equiv 1, 2, 5 \pmod 8$.

**C$_6$)** $a \equiv b \pmod m$ se, e somente se, $a + c \equiv b + c \pmod m$.

Por hipótese, $a - b = mq$, para algum inteiro $q$. Daí $(a + c) - (b + c) = mq$ e, portanto, $a + c \equiv b + c \pmod m$. Para demonstrar a recíproca, é só inverter a ordem do raciocínio.

**C$_7$)** $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $a + c \equiv b + d \pmod m$.

De fato, como $a \equiv b \pmod m$, então $a + c \equiv b + c \pmod m$, devido à propriedade anterior. Pelo mesmo motivo, da hipótese $c \equiv d \pmod m$ segue que $c + b \equiv d + b \pmod m$. Devido à transitividade: $a + c \equiv b + d \pmod m$.

Essa propriedade pode ser estendida, por indução, para $r$ congruências: se $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_r \equiv b_r \pmod m$, então:

$$a_1 + a_2 + ... + a_r \equiv b_1 + b_2 + ... + b_r \pmod m$$

Em particular, se $a_1 = a_2 = ... = a_r = a$ e $b_1 = b_2 = ... = b_r = b$:

$$ra \equiv rb \pmod m$$

**C$_8$)** Se $a \equiv b \pmod m$, então $ac \equiv bc \pmod m$.

Por hipótese, $a - b = mq$. Daí, multiplicando-se ambos os membros dessa igualdade por $c$: $ac - bc = m(qc)$. De onde $ac \equiv bc \pmod m$.

**C$_9$)** Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $ac \equiv bd \pmod m$.

Como $a \equiv b \pmod m$, então, devido à propriedade anterior, $ac \equiv bc \pmod m$. Analogamente, de $c \equiv d \pmod m$ segue que $bc \equiv bd \pmod m$. Então, devido à transitividade, $ac \equiv bc \pmod m$.

Essa propriedade pode ser generalizada, por indução, para $r$ congruências: se $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_r \equiv b_r \pmod m$, então:

$$a_1 \cdot a_2 \cdot ... \cdot a_r \equiv b_1 \cdot b_2 \cdot ... \cdot b_r \pmod{m}$$

Em particular, se $a_1 = a_2 = ... = a_r = a$ e $b_1 = b_2 = ... = b_r = b$:

$$a^r \equiv b^r \pmod{m}$$

*Exemplo 15:* Mostrar que $10^{200} - 1$ é divisível por 11.

Como $10 \equiv -1 \pmod{11}$, então, devido à propriedade anterior, $10^{200} \equiv (-1)^{200} \pmod{11}$. Ou seja, $10^{200} \equiv 1 \pmod{11}$. Daí, pela definição de congruência, $10^{200} - 1$ é divisível por 11.

*Exemplo 16:* Mostrar que, qualquer que seja o inteiro ímpar $a$, o resto da divisão de $a^2$ por 8 é 1.

Os restos possíveis da divisão de $a$ por 8 são 1, 3, 5 ou 7. (Se, por exemplo, o resto fosse 2, então $a = 8q + 2 = 2(4q+1)$ seria par, o que não é possível.)

Portanto:

$$a \equiv 1, 3, 5 \text{ ou } 7 \pmod{8}$$

Então:

$$a^2 \equiv 1, 9, 25 \text{ ou } 49 \pmod{8}$$

Mas $9 \equiv 1 \pmod{8}$, $25 \equiv 1 \pmod{8}$ e $49 \equiv 1 \pmod{8}$. Daí:

$$a^2 \equiv 1, 1, 1, \text{ ou } 1 \pmod{8}$$

Ou seja, $a^2 \equiv 1 \pmod{8}$ qualquer que seja o inteiro ímpar $a$ e, portanto, devido à propriedade $\mathbf{C_4}$, o resto da divisão de $a^2$ por 8 é 1.

**$C_{10}$)** Se $ca \equiv cb \pmod{m}$ e $\text{mdc}(c, m) = d > 0$, então $a \equiv b \pmod{m/d}$.

Por hipótese, $ca - cb = mq$, ou $c(a - b) = mq$, para algum inteiro $q$. Daí, dividindo-se os dois membros dessa igualdade por $d$, o que é possível em $\mathbb{Z}$, pois $d$ é divisor de $c$ e $m$,

$$(c/d)(a - b) = (m/d)q$$

o que mostra que $m/d$ é divisor de $(c/d)(a - b)$. Mas, por propriedade já vista, $c/d$ e $m/d$ são primos entre si. Logo, $m/d$ divide $a - b$. Isso significa que

$$a \equiv b \pmod{m/d}$$

como queríamos provar.

Por exemplo, como $14 \equiv 2 \pmod{4}$ e $\text{mdc}(2, 4) = 2$, pode-se cancelar o 2 em cada um dos números que figuram na congruência, daí resultando que $7 \equiv 1 \pmod{2}$. Convém observar, porém, que o cancelamento puro e simples do primeiro e do segundo membros não vale de um modo geral, pois, voltando-se ao exemplo considerado, $14/2 = 7$ não é côngruo a $2/2 = 1$ módulo 4. Mas há uma importante situação particular, expressa no corolário a seguir, em que vale.

**Corolário:** Se $ca \equiv cb \pmod{m}$ e $\text{mdc}(c, m) = 1$, então $a \equiv b \pmod{m}$.

A demonstração é imediata.

## 7.2 Critérios de divisibilidade

Entre outras coisas, pode-se utilizar a congruência de inteiros para estabelecer critérios de divisibilidade. Para isso é preciso usar o fato (ver **3. 3**, deste capítulo) de que todo número $N$ pode ser representado de uma única maneira como um polinômio

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_r \cdot 10^r \tag{5}$$

em que os coeficientes das potências de 10 estão sujeitos à seguinte limitação:

$$0 \leqslant a_0, a_1, a_2, \dots, a_r \leqslant 9$$

Isso dá origem à seguinte notação sequencial para indicar o número: $a_n a_{n-1} \dots a_2 a_1 a_0$. A idéia, quando se quer estabelecer um critério de divisibilidade para o número $m$, é "reduzir a expressão (5) módulo $m$". Isto é, descobrir uma expressão mais simples, em termos dos dígitos $a_1, a_2, \dots, a_r$, à qual o polinômio de (5) é côngruo, módulo $m$, e depois usar a propriedade $\mathbf{C_5}$. Vejamos alguns casos.

**(i)** *Critério de divisibilidade por 2*

Como $10^t \equiv 0 \pmod 2$, para todo $t \geqslant 1$, então $N \equiv a_0 \pmod 2$. Logo, $N$ e $a_0$ têm o mesmo resto na divisão por 2 e, em consequência, $N$ é divisível por 2 se, e somente se, $a_0$ é divisível por 2. Ou seja, se $a_0$ é par.

**(ii)** *Critério de divisibilidade por 3*

Como $10 \equiv 1 \pmod 3$, então $10^2 \equiv 1 \pmod 3$, $10^3 \equiv 1 \pmod 3$, ..., $10^r \equiv 1 \pmod 3$. Então, $a_1 \cdot 10 \equiv a_1 \pmod 3$, $a_2 \cdot 10^2 \equiv a_2 \pmod 3$, $a_3 \cdot 10^3 \equiv a_3 \pmod 3$, ..., $a_r \cdot 10^r \equiv a_r \pmod 3$.

Logo, devido às propriedades $\mathbf{C_1}$ e $\mathbf{C_7}$,

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_r \cdot 10^r \equiv a_0 + a_1 + a_2 + \dots + a_r \pmod 3$$

Portanto, $N$ e $a_0 + a_1 + a_2 + \dots + a_r$ têm o mesmo resto na divisão por 3. De onde $N$ é divisível por 3 se, e somente se, $a_0 + a_1 + a_2 + \dots + a_r$ é divisível por 3.

Por exemplo, o resto da divisão de 34567 por 3 é o mesmo da divisão de $3 + 4 + 5 + 6 + 7 = 25$ por 3, ou seja, é 1. E 34566 é divisível por 3, uma vez que $3 + 4 + 5 + 6 + 6 = 24$ o é.

**(iii)** *Critério de divisibilidade por 4*

Para esse caso cumpre observar que $10^2 \equiv 0 \pmod 4$, $10^3 \equiv 0 \pmod 4$, ..., $10^r \equiv 0 \pmod 4$. Portanto, $a_2 10^2 \equiv 0 \pmod 4$, $a_3 \cdot 10^3 \equiv 0 \pmod 4$, ..., $a_r \cdot 10^r \equiv 0 \pmod 4$. De onde:

$$N \equiv a_0 + 10a_1 \pmod 4$$

Mas $a_0 + 10a_1 = a_1 a_0$ é o número formado pelos dois últimos algarismos de $N$. Então, $N$ e $a_1 a_0$ têm o mesmo resto na divisão por 4 e, em particular, $N$ é divisível por 4 se, e somente se, $a_1 a_0$ o é.

Por exemplo o número 15424 é divisível por 4 porque 24 é divisível por 4.

**(iv)** *Critério de divisibilidade por 5*

Um número é divisível por 5 se, e somente se, seu algarismo das unidades é 0 ou 5.

A justificação fica como exercício.

**(v)** *Critério de divisibilidade por 6*

Um número é divisível por 6 se, e somente se, é divisível por 2 e 3 Se é divisível por 6 obviamente é divisível por 2 e por 3. Quanto à recíproca, é só levar em conta a proposiçao 4, uma vez que 2 e 3 são primos entre si

*Exemplo 17.* Provar que $h(n) = n(n + 1)(n + 2)$ é divisível por 6, qualquer que seja o inteiro $n$.

Provaremos que é divisível por 2 e por 3, o que é suficiente. Como $n$ ou $n + 1$ é par, então um desses números é divisível por 2 e, portanto, $h(n)$ é divisível por 2.

Por outro lado, há três possibilidades com relação ao 3:

$$n \equiv 0 \pmod 3),\ n \equiv 1 \pmod 3 \text{ ou } n \equiv 2 \pmod 3$$

No primeiro caso, $n$ é divisível por 3 e, portanto, $h(n)$ também o é; no segundo caso, somando-se 2 a ambos os membros da congruência, obtém-se $n + 2 \equiv 3 \equiv 0 \pmod 3$, o que mostra que $n + 2$ é divisível por 3 e, portanto, que $h(n)$ também é divisível por 3; e, no último caso, somando-se 1 a ambos os membros da congruência, obtém-se $n + 1 \equiv 3 \equiv 0 \pmod 3$, o que mostra que $n + 1$ é divisível por 3 e, portanto, o mesmo se pode dizer de $h(n)$. Em resumo, qualquer que seja $n$, um dos fatores de $h(n)$ é divisível por 3 e, por conseqüência, $h(n)$ também é divisível por 3.

## 8. PROBLEMA CHINÊS DO RESTO

Nosso objetivo aqui é mostrar que um sistema de congruências simultâneas do tipo

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

em que $\text{mdc}(m_i, m_j) = 1$, sempre que $i \neq j$, é *possível* (tem soluções) e determinar sua solução geral. Obviamente uma solução do sistema é um número inteiro que é solução de cada uma das congruências que o formam.

Os sistemas de congruência lineares foram introduzidos na China, em épocas remotas — talvez já fossem utilizados no século I, em questões ligadas ao calendário. Mas eles aparecem também em obras matemáticas chinesas, em versões mais simples, a mais antiga das quais é o *Manual de matemática* de Sun Tsu, escrita provavelmente do final do seculo III, e cujo conteúdo veio a se tornar parte do curso exigido para os servidores públicos civis Embora consistindo basicamente em métodos para

operações aritméticas, a obra inclui o seguinte problema, talvez o espécime mais antigo do que modernamente se chama *problema chinês do resto*:

"Temos uma certa quantidade de coisas cujo número desconhecemos. Esse número, quando dividido por 3, dá resto 2; quando dividido por 5, dá resto 3; e, quando dividido por 7, dá resto 2. Qual o número de coisas?"

Segue uma solução "por substituição" do problema. Se $N$ indica o número de coisas, então

$$N = 3x + 2$$
$$N = 5y + 3$$
$$N = 7z + 2$$

em que $x, y, z$ são números inteiros. A primeira dessas equações é equivalente à equação diofantina linear $N - 3x = 2$, cuja solução geral é

$$N = 8 - 3t, x = 2 - t \ (t \in \mathbb{Z})$$

Substituindo-se $N$ por $8 - 3t$ na segunda equação do sistema, obtém-se

$$5y + 3t = 5$$

A solução geral desta última equação diofantina é

$$y = -5 + 3s, t = 10 - 5s \ (s \in \mathbb{Z})$$

Portanto:

$$N = 8 - 3t = 8 - 3(10 - 5s) = -22 + 15s$$

Substituindo-se $N$ por $-22 + 15s$ na terceira equação do sistema, obtém-se

$$7z - 15s = -24$$

cuja solução geral é

$$z = 48 - 15r, s = 24 - 7r \ (r \in \mathbb{Z})$$

De onde,

$$N = -22 + 15s = -22 + 15(24 - 7r) = 338 - 105r \ (r \in \mathbb{Z})$$

que é a solução geral do problema.

Sun Tsu, que provavelmente desconhecia um método geral para resolver esse problema e, portanto, devia ignorar que ele tem uma infinidade de soluções, só encontrou a solução 23, número correspondente a $r = 3$ na solução geral.

**Proposição 8** (teorema chinês do resto): Sejam $m_1, m_2, ..., m_r$ números inteiros maiores que 1 e tais que $\text{mdc}(m_i, m_j) = 1$, sempre que $i \neq j$. Assim sendo, se $a_1, a_2, ..., a_n$ são números inteiros arbitrários, então o sistema de congruências

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

é possível. Ademais, duas soluções quaisquer do sistema são côngruas módulo $m_1m_2...m_r$.

*Demonstração:* As características do sistema sugerem que um número que possa ser escrito como

$$y_1a_1 + y_2a_2 + ... + y_ra_r$$

em que $y_1 \equiv 1 \pmod{m_1}$, $y_1 \equiv 0 \pmod{m_i} (i \neq 1)$; $y_2 \equiv 1 \pmod{m_2}$, $y_2 \equiv 0 \pmod{m_i} (i \neq 2)$, e assim por diante, é uma solução do sistema. Mostremos, por exemplo, que ele é solução da segunda congruência. Como $y_1, y_3, ..., y_r \equiv 0 \pmod{m_2}$, então $y_1a_1 + y_3a_3 + ... + y_ra_r \equiv 0 \pmod{m_2}$. Como $y_2 \equiv 1 \pmod{m_2}$, então $y_2a_2 \equiv a_2 \pmod{m_2}$. Portanto, $y_1a_1 + y_2a_2 + ... + y_ra_r \equiv a_2 \pmod{m_2}$.

Para encontrar um sistema de números que cumpra o papel dos $y_i$ $(i = 1, 2, ..., r)$ façamos $m_1m_2...m_r = m$. Então $\text{mdc}(m_1, m/m_1) = 1$, pois um divisor primo de $m_1$ e $m/m_1$ teria também de ser divisor de algum $m_j$, com $j \neq 1$, o que é impossível, pela hipótese.

Portanto, a congruência linear

$$(m/m_1)y \equiv 1 \pmod{m_1}$$

tem solução. Se $b_1$ é uma de suas soluções, então:

$$(m/m_1)b_1 \equiv 1 \pmod{m_1}$$

Mas, como $m_2, m_3, ..., m_r$ são divisores de $m/m_1$, então $m/m_1 \equiv 0 \pmod{m_2}$, $m/m_1 \equiv 0 \pmod{m_3}$, ..., $m/m_1 \equiv 0 \pmod{m_r}$ e, portanto, $(m/m_1)b_1 \equiv 0 \pmod{m_2}$, $(m/m_1)b_1 \equiv 0 \pmod{m_3}$, ..., $(m/m_1)b_1 \equiv 0 \pmod{m_r}$. Analogamente, se $b_2$ é solução de $(m/m_2)y \equiv 1 \pmod{m_2}$, então $(m/m_2)b_2 \equiv 1 \pmod{m_2}$ e $(m/m_2)b_2 \equiv 0 \pmod{m_1}$, $(m/m_2)b_2 \equiv 0 \pmod{m_3}$, ..., $(m/m_r)b_2 \equiv 0 \pmod{m_r}$. E assim por diante. Portanto $(m/m_1)b_1, (m/m_2)b_2, ..., (m/m_r)b_r$ cumprem o papel exigido para os números $y_1, y_2, ..., y_r$, conforme colocação inicial, e

$$b = (m/m_1)b_1a_1 + (m/m_2)b_2a_2 + ... + (m/m_r)b_ra_r$$

é uma solução do sistema.

Se $c$ é uma outra solução, então $c \equiv b \pmod{m_i}$ $(i = 1, 2, ..., r)$. Portanto $m_1, m_2, ..., m_r$ são divisores de $c - b$. Mas, como $m_1, m_2, ..., m_r$ são primos entre si, dois a dois, então $m_1m_2...m_r$ também é um divisor de $c - b$. De onde $c \equiv b \pmod{m_1m_2...m_r}$. Portanto, a solução geral do sistema é

$$x \equiv b \pmod{m_1m_2...m_r} \qquad \#$$

*Exemplo 18:* O teorema anterior é construtivo, como se nota pela demonstração. Vejamos como utilizá-la na resolução do sistema

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Nesse caso, $m = 30$ e as congruências lineares a resolver são $15y \equiv 1 \pmod 2$, $10y \equiv 1 \pmod 3$ e $6y \equiv 1 \pmod 5$. Como o número 1 é solução particular de cada uma delas, então uma solução do sistema é $15 \cdot 1 \cdot 1 + 10 \cdot 1 \cdot 2 + 6 \cdot 1 \cdot 3 = 53$. Logo a solução geral do sistema é dada por

$$x \equiv 53 \equiv 23 \pmod{30}$$

## Exercícios

**38.** Ache os restos das seguintes divisões:

a) $2^{45}$ por 7

b) $11^{100}$ por 100

c) $3^{10} \cdot 42^5 + 6^8$ por 5

d) $5^2 \cdot 4841 + 28^5$ por 3

**Resolução**

c) Como $3 \equiv -2 \pmod 5$, então $3^2 \equiv 4 \pmod 5$, $3^3 \equiv -8 \equiv 2 \pmod 5$, $3^4 = 16 \equiv 1 \pmod 5$ daí para a frente os resultados se repetem ciclicamente de quatro em quatro. Como $10 \equiv 2 \pmod 4$, então $3^{10} \equiv 4 \pmod 5$. Por outro lado, como $42 \equiv 2 \pmod 5$, então $42^2 \equiv 4 \equiv -1 \pmod 5$, $42^3 \equiv -2 \pmod 5$, $42^4 \equiv (-1)^2 \equiv 1 \pmod 5$, e daí para a frente os resultados se repetem também de quatro em quatro. Observando-se que $5 \equiv 1 \pmod 4$, deduz-se $42^5 \equiv 2 \pmod 5$. Por último, como $6 \equiv 1 \pmod 5$, então $6^8 \equiv 1 \pmod 5$. Juntando as conclusões parciais:

$$3^{10} \cdot 42^5 + 6^8 \equiv 4 \cdot 2 + 1 \equiv 4 \pmod 5$$

Portanto, o resto é 4. ■

**39.** Mostre que o número $2^{20} - 1$ é divisível por 41.

**40.** Qual é o resto da divisão euclidiana de $1^5 + 2^5 + 3^5 + ... + 99^5 + 100^5$ por 4? Justifique.

*Sugestão:* Dividir a soma dada em 25 grupos de 4 parcelas.

**41.** a) Mostre que o resto da divisão de um número por 10 é seu algarismo das unidades e que o resto da divisão por 100 é o número formado pelo dois últimos algarismos do número dado.

b) Ache o algarismo das unidades de $7^{(7^{100})}$.

c) Ache os dois últimos algarismos de $9^{(9^9)}$.

**Resolução**

a) Seja $N$ um inteiro positivo. Como já vimos, pode-se representar $N$ pela expressão

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_r \cdot 10^r \ (0 \leqslant a_0, a_1, ..., a_r \leqslant 9)$$

Daí seguem duas possibilidades de escrever o número $N$: $N = a_0 + 10 \cdot q$ (quando se põe 10 em evidência nas $r$ últimas parcelas do segundo membro) e $N = a_0 + a_1 \cdot 10 + 100 \cdot q$ (quando se põe 100 em evidência nas $r - 1$ últimas parcelas do segundo membro). A primeira igualdade mostra que o resto da divisão de $N$ por 10 é $a_0$, o algarismo das unidades de $N$. E a segunda que o resto da divisão de $N$ por 100 é $a_0 + a_1 \cdot 10$, número formado pelos dois últimos algarismos de $N$ (por quê?)

As partes b) e c) ficam apenas propostas. ■

**42.** Se $p$ e $p + 2$ são números primos, então eles se denominam *primos gêmeos*. É o caso, por exemplo, de 3 e 5.

Se $p > 3$ e os números $p$ e $p + 2$ são primos gêmeos, prove que a soma $p + (p + 2) = 2p + 2$ é múltiplo de 12.

*Sugestão:* Sendo a soma um número par, então a princípio essa soma poderia ser côngrua a 0, 2, 4, 6 , 8, 10 módulo 12. Mostrar que todas essas possibilidades, exceto a primeira, levam a uma contradição.

**43.** Prove que se $a \equiv b \pmod{m}$ e $n$ é um divisor de $m$, maior que 1, então $a \equiv b \pmod{n}$.

**44.** Demonstre:

a) $a^3 \equiv a \pmod{6}$

b) $a^3 \equiv 0, 1$ ou $8 \pmod{9}$

c) Se $a$ é um inteiro que não é divisível por 2 nem por 3, então $a^2 \equiv 1 \pmod{24}$.

d) Se $a$ é um cubo perfeito, então $a \equiv 0, 1$ ou $-1 \pmod{9}$.

**Resolução**

d) Por hipótese, $a = b^3$ para algum inteiro $b$. Mas $b \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4 \pmod{9}$. Portanto $b^3 \equiv 0, \pm 1, \pm 8, \pm 27, \pm 64 \pmod{9}$. Como $8 \equiv -1 \pmod{9}$, $-8 \equiv 1 \pmod{9}$, $27 \equiv 0 \pmod{9}$, $-27 \equiv 0 \pmod{9}$, $64 \equiv 1 \pmod{9}$ e $-64 \equiv -1 \pmod{9}$, então $a = b^3 \equiv 0, 1$ ou $-1 \pmod{9}$. Isso significa que o resto da divisão de um cubo perfeito por 9 é 0, 1 ou 8 (que corresponde a $-1$). ∎

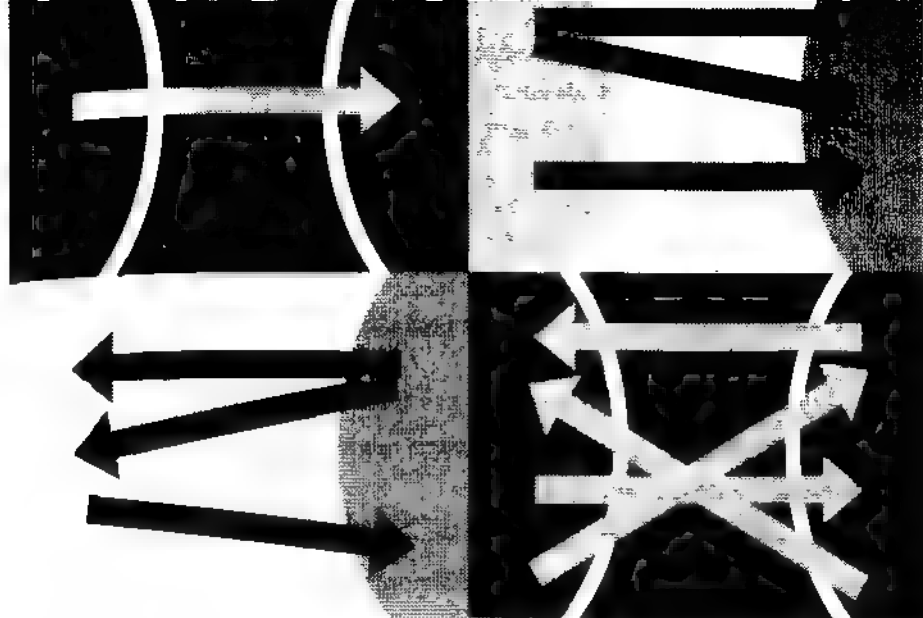
**45.** a) Encontre um inteiro $x$ tal que $x \equiv 3 \pmod{10}$, $x \equiv 11 \pmod{13}$ e $x \equiv 15 \pmod{17}$ (Regiomantanus, século XVI).

b) Encontre um inteiro $x$ tal que $x \equiv 3 \pmod{11}$, $x \equiv 5 \pmod{19}$ e $x \equiv 10 \pmod{29}$ (Euler, século XVIII).

**46.** Resolva, mediante o teorema chinês do resto, os seguintes sistemas:

a) $x \equiv 1 \pmod{10}$, $x \equiv 4 \pmod{11}$, $x \equiv 6 \pmod{13}$

b) $x \equiv 5 \pmod{7}$, $x \equiv -1 \pmod{9}$, $x \equiv 6 \pmod{10}$

**47.** Um bando de 17 piratas, ao tentar dividir igualmente entre si as moedas de uma arca, verificou que haveria uma sobra de 3 moedas. Seguiu-se uma discussão, na qual um pirata foi morto. Na nova tentativa de divisão, já com um pirata a menos, verificou-se que haveria uma sobra de 10 moedas. Nova confusão, e mais um pirata foi morto. Então, por fim, eles conseguiram dividir igualmente as moedas entre si. Qual o menor número de moedas que a arca poderia conter?

CAPÍTULO III

# RELAÇÕES, APLICAÇÕES, OPERAÇÕES

## III–1 RELAÇÕES BINÁRIAS

### 1. CONCEITOS BÁSICOS

#### 1.1 Produto cartesiano

**Definição 1:** Dados dois conjuntos, $E$ e $F$, não vazios, chama-se *produto cartesiano de* E *por* F o conjunto formado por todos os pares ordenados $(x, y)$, com $x$ em $E$ e $y$ em $F$.

O conceito de *par ordenado* é tomado aqui como primitivo, postulando-se que $(x, y) = (u, v)$ se, e somente se, $x = u$ e $y = v$.

Costuma-se indicar o produto cartesiano de $E$ por $F$ com a notação $E \times F$ (lê-se "$E$ cartesiano $F$"). Assim, temos:

$$E \times F = \{(x, y) \mid x \in E \text{ e } y \in F\}$$

#### 1.2 Relação binária

Na matemática, e ate no dia-a-dia, temos de lidar frequentemente com "relações" entre elementos de um conjunto $E$ ou entre elementos de dois conjuntos distintos, $E$ e $F$.

Por exemplo, se $E$ indica os membros de uma família (pais e filhos, apenas), são relações entre elementos de $E$:

• "$x$ é irmão de $y$";

• "$x$ é pai de $y$".

No terreno da matemática, se $E = F = \mathbb{R}$ (conjunto dos números reais), são "relações" entre elementos de $\mathbb{R}$:

• a igualdade ($x = y$);

• a desigualdade ($x \neq y$);

• "$x$ é menor que $y$" ($x < y$);

• $x + y = 10$.

Para outro exemplo, consideremos $E = \{0, 1, 2, 3, ...\}$ e $F = \{..., -3, -2, -1\}$. Então, é uma relação entre elementos de $E$ e $F$:

• $x + y = 0$, em que $x$ representa um elemento de $E$ e $y$ um elemento de $F$.

De situações como essa, decorre naturalmente uma idéia informal de "relação": é um sistema $R$ constituído de:

1) um conjunto $E$ (chamado *conjunto de partida*)

2) um conjunto $F$ (chamado *conjunto de chegada*);

3) uma sentença aberta $p(x, y)$, em que $x$ é uma variável em $E$ e $y$ uma variável em $F$, sentença essa tal que, para todo par ordenado $(a, b) \in E \times F$, a proposição $p(a, b)$ é verdadeira ou falsa.

Quando $p(a, b)$ é verdadeira, diz se que "a *está relacionado com* b *mediante* (ou *através de*) R" e escreve-se

$$aRb$$

Se $p(a, b)$ é falsa, diz-se que "a *não está relacionado com* b *mediante* (ou *através de*) R" e escreve-se

$$a \not R b$$

Por exemplo, se $R$ indica a relação em que o conjunto de partida e o conjunto de chegada são iguais a $\mathbb{R}$ e a função proposicional é $x^2 + y = 0$, então

$$1R(-1), (-3)R(-9) \text{ e } 0R0$$

ao passo que

$$0 \not R 1, (-1) \not R (-4) \text{ e } 3 \not R 6$$

O conjunto dos elementos $a \in E$ tais que $aRb$, para pelo menos um elemento $b \in F$, é chamado *domínio* da relação e é denotado por $D(R)$. E o conjunto dos elementos $b \in F$ tais que, para pelo menos um elemento $a \in E$, verifica-se $aRb$, é chamado *conjunto imagem* da relação e é denotado por $\text{Im}(R)$.

Por exemplo, considere a relação "ser pai de" numa família constituída de 5 membros: o pai é $a$, a mãe é $b$, e os filhos $m$, $n$ e $r$. Nesse caso, podemos considerar o

conjunto de partida e o conjunto de chegada iguais a $\{a, b, m, n, r\}$. Obviamente o domínio da relação considerada é $\{a\}$ e o conjunto imagem é $\{m, n, r\}$.

Outro exemplo: se indicarmos por $R$ a relação que tem como conjunto de partida $\{0, 1, 2, 3, ...\}$, conjunto de chegada $\{..., -3, -2, -1\}$ e função proposicional dada por $y = -2x$, então $D(R) = \{1, 2, 3, ...\}$, ao passo que $Im(R) = \{-2, -4, -6, ...\}$

Segue uma definição mais precisa da relação, usando-se apenas a linguagem de conjuntos

**Definição 2:** Chama-se *relação binária de* E *em* F todo subconjunto $R$ de $E \times F$. Logo.

$$(R \text{ é relação de } E \text{ em } F) \text{ se, e somente se, } R \subset E \times F$$

Conforme essa definição, $R$ é um conjunto de pares ordenados $(a, b)$ pertencentes a $E \times F$.

Para indicar que $(a, b) \in R$, usaremos algumas vezes a notação

$$aRb$$

(lê-se "*a* erre *b*" ou "*a* relaciona-se com *b* segundo *R*").

Se $(a, b) \notin R$, escreveremos $a\not{R}b$.

Os conjuntos $E$ e $F$ são denominados, respectivamente, *conjunto de partida* e *conjunto de chegada* da relação $R$.

Vale notar que essa definição pode ser considerada equivalente à idéia de relação dada no início, desde que admitamos a existência, para cada parte $R$ de $E \times F$, de uma função proposicional $p(x, y)$, com $x$ é variável em $E$ e $y$ é variável em $F$, função essa que tem como conjunto verdade $R$.

No que segue, até por simplicidade, ao considerar ou ao nos referirmos a uma relação $R$, estaremos pressupondo a definição 2.

*Exemplos 1:*

1º) Se $E = \{0, 1, 2, 3\}$ e $F = \{4, 5, 6\}$, então:

$$E \times F = \{(0, 4), (0, 5), (0, 6), (1, 4), (1, 5), (1, 6), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)\}$$

Qualquer subconjunto de $E \times F$ é uma relação de $E$ em $F$. São exemplos de relações:

$$\varnothing$$
$$R_1 = \{(0, 4), (0, 5), (0, 6)\}$$
$$R_2 = \{(0, 4), (1, 4), (1, 5), (2, 6)\}$$
$$R_3 = \{(2, 5), (3, 6)\}$$

2º Se $E = F = \mathbb{Z}$, então $E \times F$ é o conjunto formado por todos os pares ordenados de numeros inteiros. Um exemplo de relação de $\mathbb{Z}$ em $\mathbb{Z}$ é.

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = -y\}$$
$$= \{..., (-n, n), ..., (-2, 2), (-1, 1), (0, 0), (1, -1), ..., (n, -n), ...\}$$

3º) Se $E = F = \mathbb{R}$, então $E \times F$ é o conjunto formado por todos os pares ordenados de números reais. Um exemplo de relação de $\mathbb{R}$ em $\mathbb{R}$ é:

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq 0 \text{ e } y \geq 0\}$$

## 1.3 Domínio e imagem

Seja $R$ uma relação de $E$ em $F$.

**Definição 3:** Chama-se *domínio* de $R$ o subconjunto de $E$ constituído pelos elementos $x$ para cada um dos quais existe algum $y$ em $F$ tal que $x\,R\,y$

$$D(R) = \{x \in E \mid \exists\ y \in F : xRy\}$$

**Definição 4:** Chama-se *imagem* de $R$ o subconjunto de $F$ constituído pelos elementos $y$ para cada um dos quais existe algum $x$ em $E$ tal que $x\,R\,y$.

$$Im(R) = \{y \in F \mid \exists\ x \in E : xRy\}$$

Em outros termos, $D(R)$ é o conjunto formado pelos primeiros termos dos pares ordenados que constituem $R$ e $Im(R)$ é formado pelos segundos termos dos pares de $R$.

Assim, voltando aos exemplos anteriores, temos:

1º) $D(R_1) = \{0\}$ e $Im(R_1) = \{4, 5, 6\}$

$D(R_2) = \{0, 1, 2\}$ e $Im(R_2) = \{4, 5, 6\}$

$D(R_3) = \{2, 3\}$ e $Im(R_3) = \{5, 6\}$

2º) $D(R) = \mathbb{Z}$ e $Im(R) = \mathbb{Z}$

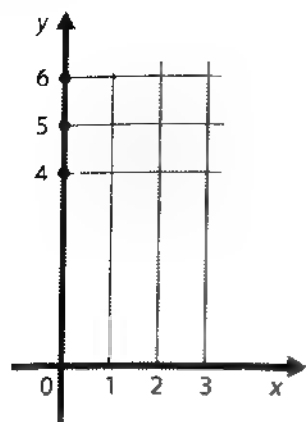
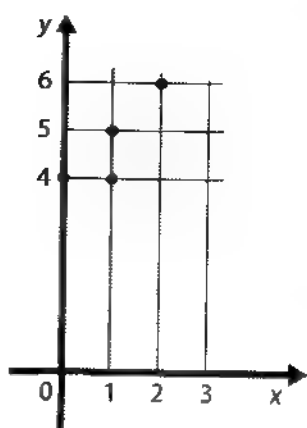
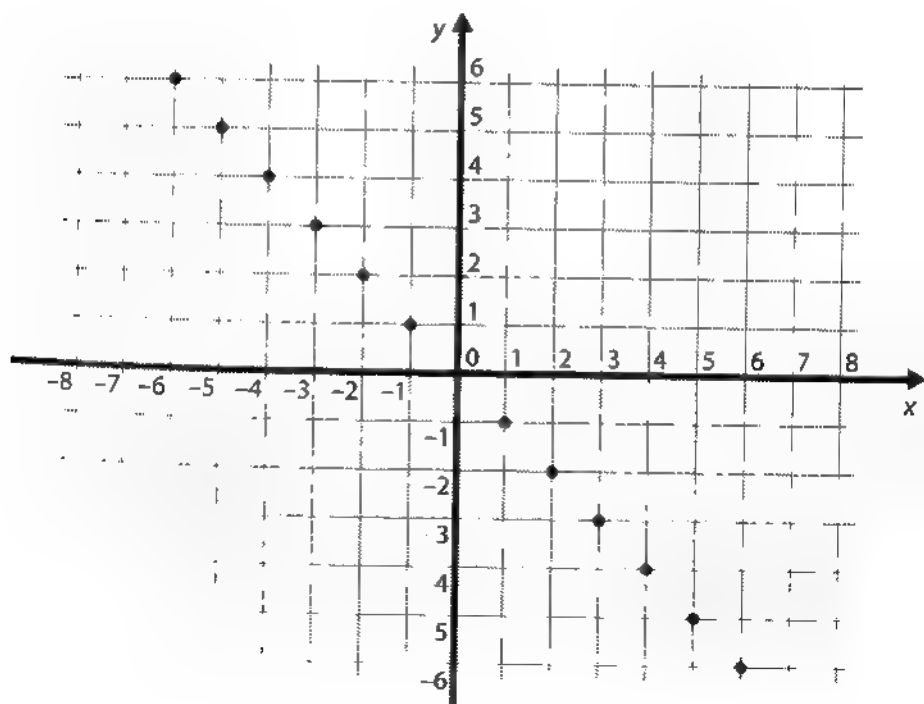
3º) $D(R) = \mathbb{R}_+$ e $Im(R) = \mathbb{R}_+$

## 1.4 Representações

### a) Gráfico cartesiano

Grande parte das relações estudadas em matemática são relações em que $E$ (conjunto de partida) e $F$ (conjunto de chegada) são subconjuntos de $\mathbb{R}$. Nesses casos, o gráfico cartesiano da relação é o conjunto dos pontos de um plano dotado de um sistema de coordenadas cartesianas ortogonais, cujas abscissas são os primeiros termos e as ordenadas os segundos termos dos pares que constituem a relação.

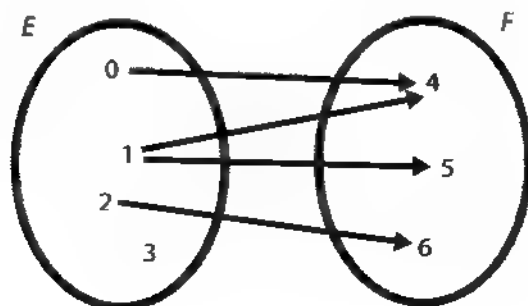
*Exemplos 2:*

1º) $R_1 = \{(0, 4), (0, 5), (0, 6)\}$

$R_2 = \{(0, 4), (1, 4), (1, 5), (2, 6)\}$

2º) $E = \mathbb{Z}$, $F = \mathbb{Z}$ e $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = -y\}$

3°) $E = \mathbb{R}$, $F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq 0 \text{ e } y \geq 0\}$

**b) Esquema de flechas**

Quando $E$ e $F$ são conjuntos finitos com "poucos" elementos, podemos indicar uma relação de $E$ em $F$ da seguinte forma: representamos $E$ e $F$ por meio de diagramas de Venn e indicamos cada $(x, y) \in \mathbb{R}$ por uma flecha com "origem" $x$ e "extremidade" $y$.

*Exemplo 3:*

$E = \{0, 1, 2, 3\}$
$F = \{4, 5, 6\}$
$R = \{(0, 4), (1, 4), (1, 5), (2, 6)\}$

## 1.5 Inversa de uma relação

**Definição 5:** Seja $R$ uma relação de $E$ em $F$. Chama-se *relação inversa* de $R$, e indica-se por $R^{-1}$, a seguinte relação de $F$ em $E$:

$$R^{-1} = \{(y, x) \in F \times E \mid (x, y) \in R\}$$

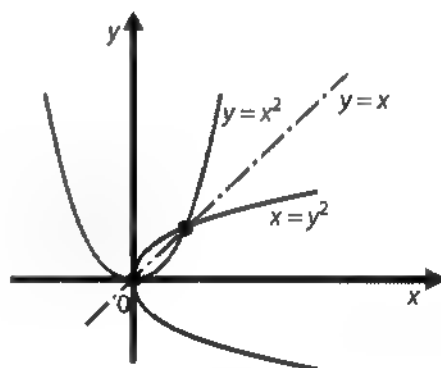
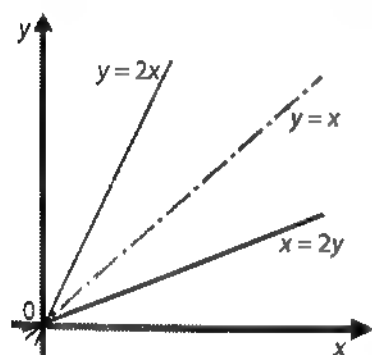
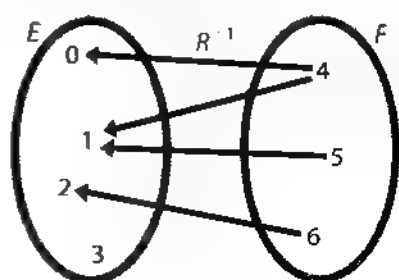
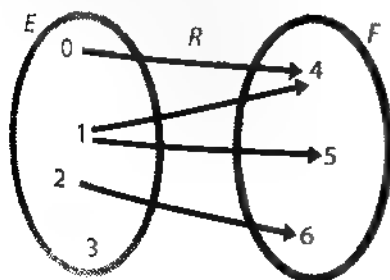
*Exemplos 4:*

1º) $E = \{0, 1, 2, 3\}$, $F = \{4, 5, 6\}$ e $R = \{(0, 4), (0, 5), (0, 6)\}$, então:
$R^{-1} = \{(4, 0), (5, 0), (6, 0)\}$

2º) $E = \mathbb{R}$, $F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R}^2 \mid y = 2x\}$, então:
$R^{-1} = \{(y, x) \in \mathbb{R}^2 \mid y = 2x\} = \{(x, y) \in \mathbb{R}^2 \mid x = 2y\}$

3º) $E = \mathbb{R}$, $F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$, então:
$R^{-1} = \{(y, x) \in \mathbb{R}^2 \mid y = x^2\} = \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$

**Representação de $R^{-1}$**

a) Se a relação $R$ admite um gráfico cartesiano, então o mesmo ocorre com $R^{-1}$. Notando-se que $(x, y) \in \mathbb{R}$ se, e somente se, $(y, x) \in R^{-1}$, então o gráfico de $R^{-1}$ é simétrico do gráfico de $R$ relativamente à reta de equação $y = x$. Exemplos:

b) Dado o diagrama de Euler-Venn de uma relação $R$, obtemos o diagrama de $R^{-1}$ simplesmente invertendo o sentido das flechas. Por exemplo, se $E = \{0, 1, 2, 3\}$, $F = \{4, 5, 6\}$ e $R = \{(0, 4), (1, 4), (1, 5), (2, 6)\}$, temos:

isto é, $R^{-1} = \{(4, 0), (4, 1), (5, 1), (6, 2)\}$.

**Propriedades:** Decorrem diretamente da definição de relação inversa as propriedades seguintes:

a) $D(R^{-1}) = Im(R)$

b) $Im(R^{-1}) = D(R)$

c) $(R^{-1})^{-1} = R$

### Exercícios

**1.** Sejam $E = \{1, 3, 5, 7, 9\}$ e $F = \{0, 2, 4, 6\}$.

a) Enumere os elementos das seguintes relações de $E$ em $F$:

$R_1 = \{(x, y) \mid y = x - 1\}$
$R_2 = \{(x, y) \mid x < y\}$
$R_3 = \{(x, y) \mid y = 3x\}$

b) Estabeleça o domínio e a imagem de cada uma.

**2.** Sabe-se que $E$ é um conjunto com 5 elementos e $R = \{(a, b), (b, c), (c, d), (d, e)\}$ é uma relação sobre $E$. Pede-se obter:

a) os elementos de $E$;

b) domínio e imagem de $R$;

c) os elementos, domínio e imagem de $R^{-1}$;

d) esquema de flechas de $R$.

**3.** Sendo $R = \{(x, y) \mid 4x^2 + y^2 = 4\}$ uma relação sobre $\mathbb{R}$, pede-se:

a) o gráfico cartesiano de $R$;

b) o domínio de $R$;

c) a imagem de $R$;

d) descrever $R^{-1}$.

**4.** Seja $R$ a relação sobre o conjunto $\mathbb{N}^*$ definida pela sentença $x + 3y = 10$. Pede-se determinar:

a) os elementos de $R$;

b) o domínio de $R$;

c) a imagem de $R$;

d) os elementos de $R^{-1}$.

**5.** Sejam $E$ e $F$ dois conjuntos finitos com $m$ e $n$ elementos, respectivamente.

a) Qual é o número de elementos de $E \times F$?

b) Qual é o número de relações de $E$ em $F$?

**6.** Seja $R$ uma relação binária sobre o conjunto $E$ e $R'$ a negação de $R$, isto é, $R' = \{(x, y) \mid x \not R y\}$. O que se pode concluir sobre $R \cap R'$ e $R \cup R'$?

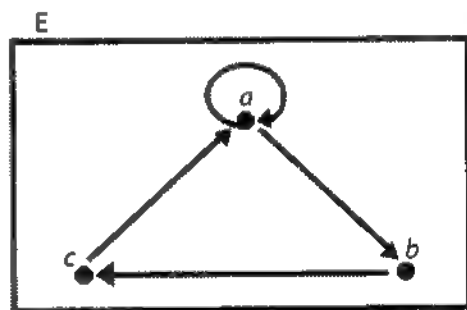
**7.** Sejam $R_1$ e $R_2$ duas relações binárias em $E$. Que significado têm $R_1 \cup R_2$ e $R_1 \cap R_2$? O que significa a inclusão $R_1 \subset R_2$?

## 1.6 Relação sobre um conjunto

**Definição 6:** Quando $E = F$ e $R$ é uma relação de $E$ em $F$, diz-se que $R$ é uma *relação sobre* E ou, ainda, $R$ é uma *relação em* E.

As relações sobre $E$ vão merecer um destaque especial neste livro. Veremos algumas propriedades que as relações sobre $E$ podem apresentar e, em seguida, estudaremos dois tipos de relações sobre $E$ extremamente importantes: as relações de equivalência e as relações de ordem.

No estudo das relações sobre $E$, em que $E$ é conjunto finito com "poucos" elementos, é muito útil a representação através do esquema de flechas, que pode ser assim simplificado: representamos os elementos de $E$ por pontos de um retângulo e indicamos cada par $(a, b)$ da relação através de uma flecha com "origem" $a$ e "extremidade" $b$. No caso de $(a, a)$ estar na relação, usa-se um "laço" envolvendo $a$, conforme mostra o exemplo a seguir.

*Exemplo 5:* O esquema ao lado representa a relação $R = \{(a, a), (a, b), (b, c), (c, a)\}$ sobre $E = \{a, b, c\}$.

## 1.7 Propriedades

Daremos a seguir as principais propriedades que uma relação $R$ sobre $E$ pode verificar.

### a) Reflexiva

**Definição 7:** Dizemos que $R$ é *reflexiva* quando todo elemento de $E$ se relaciona consigo mesmo. Ou seja, quando, para todo $x \in E$, vale $xRx$.

Se designarmos por $\Delta_E$ o conjunto de todos os pares $(x, x)$, com $x \in E$, então $R$ é reflexiva quando $\Delta_E \subset R$.

*Exemplos 6:*

1º) A relação $R = \{(a, a), (b, b), (c, c), (a, b), (b, c)\}$ sobre $E = \{a, b, c\}$ é reflexiva, pois $aRa$, $bRb$ e $cRc$.

2º) A relação $R$ de igualdade sobre o conjunto $\mathbb{Z}$ dos números inteiros $xRy$ se, e somente se, $x = y$ é reflexiva pois $x = x$, para todo $x \in \mathbb{Z}$.

3º) A relação $R$ de paralelismo definida sobre o conjunto $E$ das retas do espaço euclidiano $xRy$ se, e somente se, $x \parallel y$ é reflexiva, pois $x \parallel x$, para toda reta $x$.

*Contra-exemplo 1:*

Notemos que uma relação $R$ sobre $E$ *não é reflexiva* quando existe um elemento $x$ em $E$ tal que $x \not R x$.

Assim, por exemplo, a relação

$R = \{(a, a), (a, b), (b, a), (b, b), (b, c)\}$ sobre $E = \{a, b, c\}$ não é reflexiva, pois $c \not R c$.

**b) Simétrica**

**Definição 8:** Dizemos que $R$ é *simétrica* se vale $yRx$ sempre que vale $xRy$. Ou seja, se $xRy$, então $yRx$.

*Exemplos 7.*

1º) A relação $R = \{(a, a), (a, b), (b, a), (c, c)\}$ é uma relação simétrica sobre $E = \{a, b, c\}$.

2º) A relação $R$ de perpendicularismo definida sobre o conjunto $E$ das retas do espaço

$$xRy \text{ se, e somente se, } x \perp y$$

é simétrica, pois, para duas retas $x$ e $y$ quaisquer, $x \perp y \Rightarrow y \perp x$

3º) A relação $R$ sobre o conjunto $\mathbb{Q}$ dos números racionais, definida por

$$xRy \text{ se, e somente se, } x^2 = y^2$$

é simétrica, pois, para dois racionais $x$ e $y$ quaisquer, $x^2 = y^2 \Rightarrow y^2 = x^2$.

*Contra-exemplo 2:*

Notemos que uma relação $R$ sobre $E$ não é simétrica se existirem $x$ e $y$ em $E$ tais que $xRy$ e $y \not R x$.

Assim, por exemplo, a relação

$R = \{(a, a), (a, b), (b, b), (c, c)\}$ sobre $E = \{a, b, c\}$ não é simétrica, pois $aRb$ e $b \not R a$.

**c) Transitiva**

**Definição 9:** Dizemos que $R$ é transitiva se vale $xRz$ sempre que vale $xRy$ e $xRz$. Ou seja, se $xRy$ e $xRz$, então $xRz$.

*Exemplos 8:*

1º) A relação $R = \{(a, b), (b, b), (b, c), (a, c), (c, c)\}$ sobre $E = \{a, b, c\}$ é transitiva.

2°) A relação $R$ de semelhança ($\sim$) definida sobre o conjunto $E$ dos triângulos do espaço

$$xRy \text{ se, e somente se, } x \sim y$$

é transitiva, pois, sendo $x$, $y$ e $z$ triângulos quaisquer, tem se.

$$x \sim y \text{ e } y \sim z \Rightarrow x \sim z$$

3º) A relaçao $R$ sobre o conjunto $\mathbb{N}$ dos números naturais definida por

$$xRy \text{ se, e somente se, } x \leqslant y$$

e transitiva, pois, dados três naturais $x$, $y$ e $z$, tem-se.

$$x \leqslant y \text{ e } y \leqslant z \Rightarrow x \leqslant z$$

*Contra-exemplo 3:*

Notemos que uma relação $R$ sobre $E$ *não* é transitiva se existirem $x$, $y$ e $z$ em $E$ tais que $xRy$, $yRz$ e $x\not{R}z$.

Assim, por exemplo, a relação

$R = \{(a, a), (a, b), (b, c), (c, c)\}$ sobre $E = \{a, b, c\}$

não é transitiva, pois $aRb$, $bRc$ e $a\not{R}c$.

Da mesma forma, a relação

$S = \{(a, b), (b, a)\}$ sobre $E = \{a, b, c\}$ não é transitiva, pois $aSb$, $bSa$ e $a\not{S}a$.

**d) Anti-simétrica**

**Definição 10:** Dizemos que $R$ é *anti-simétrica* se $x = y$, sempre que $xRy$ e $yRx$. Ou seja, se $xRy$ e $yRx$, então $x = y$.

É importante destacar a contrapositiva da definição10: se $x \neq y$, então $x\not{R}y$ ou $y\not{R}x$.

*Exemplos 9:*

1º) A relação $R = \{(a, a), (a, b), (b, c), (c, a)\}$ sobre $E = \{a, b, c\}$ é anti-simétrica.

2º) A relação $R$ de divisibilidade sobre o conjunto N dos números naturais

$$xRy \text{ se, e somente se, } x \mid y \text{ (lê-se ``}x\text{ é divisor de }y\text{'')}$$

é anti-simétrica, pois, dados dois números naturais, $x$ e $y$ se $x \mid y$ e $y \mid x$, então $x = y$.

3º) A relação $R$ sobre o conjunto $\mathbb{R}$ dos números reais dada por

$$xRy \text{ se, e somente se, } x \leqslant y$$

e anti-simétrica, pois, sendo $x$ e $y$ números reais quaisquer, se $x \leqslant y$ e $y \leqslant x$, então $x = y$.

*Contra exemplos 4:*

Notemos que uma relação $R$ sobre $E$ *nao* é anti-simétrica se existirem $x$ e $y$ em $E$ tais que $x \neq y$ e $xRy$ e $yRx$

$R = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$ sobre $E = \{a, b, c\}$

nao é anti simétrica, pois $b \neq c$, $bRc$ e $cRb$.

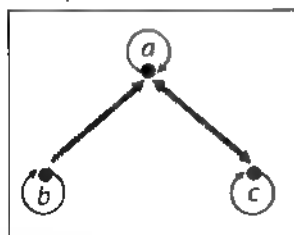
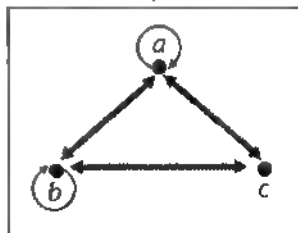
Outro contra-exemplo: a relação $R$ de divisibilidade sobre o conjunto $\mathbb{Z}$ dos números inteiros não é anti-simétrica, pois $2 \neq \ \ 2, 2 \mid \ \ 2$ e $\ \ 2 \mid 2$

## 1.8 Diagrama de flechas e propriedades

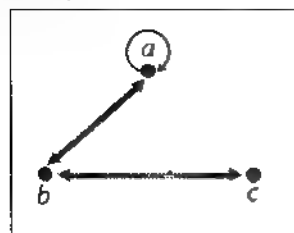
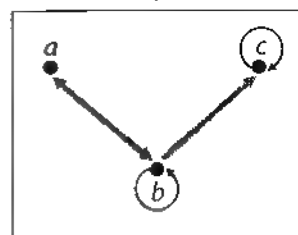
Quando $E$ é finito e tem "poucos" elementos, é possível visualizar se uma relação $R$ sobre $E$ goza ou não das propriedades definidas no item anterior observando-se o diagrama de flechas de $R$.

**Reflexiva**

Em cada ponto do diagrama deve haver um laço.

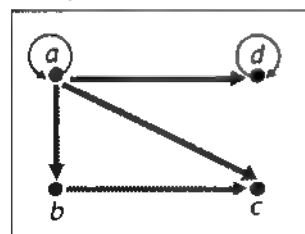
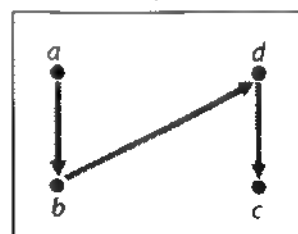
Exemplo:

Contra-exemplo:

**Simétrica**

Toda flecha tem duas "pontas".

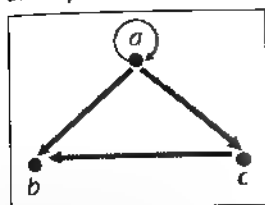
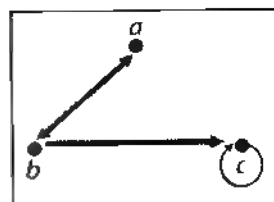
Exemplo:

Contra exemplo:

**Transitiva**

Para todo par de flechas consecutivas existe uma terceira flecha cuja origem é a origem da primeira e a extremidade, a da segunda.

Exemplo:

Contra-exemplo:

**Anti-simétrica**

Não há flechas de duas pontas.

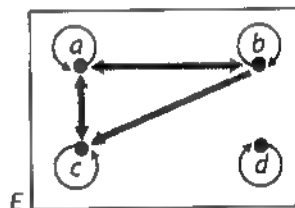
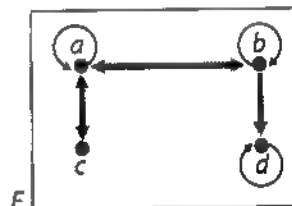
Exemplo:

Contra exemplo:

## Exercícios

**8.** Seja $R$ a relação em $E = \{1, 2, 3, 4, 5\}$ tal que $xRy$ se, e somente se, $x - y$ é múltiplo de 2.

a) Quais são os elementos de $R$?

b) Faça o diagrama de flechas para $R$.

c) $R$ é reflexiva? $R$ é simétrica? $R$ é transitiva? $R$ é anti-simétrica?

**9.** $R$ é uma relação sobre $E = \{a, b, c, d\}$ dada pelo esquema de flechas ao lado. Que propriedades $R$ apresenta?

**10.** Que propriedades apresenta a relação $S$ dada pelo esquema ao lado?

**11.** O conjunto $E = \{a, b, c, d, e\}$ é formado pelos cinco filhos de um mesmo casa

Seja $R$ a relação sobre $E$ assim definida:

$xRy$ se, e somente se, $x$ é irmão de $y$

Que propriedades $R$ apresenta?

*Nota.* $x$ é irmão de $y$ quando $x \neq y$ e $x$ e $y$ têm os mesmos pais.

**12.** Seja $E$ o conjunto das retas que contêm os lados de um hexágono regular *abcde*

a) Quantos elementos tem o conjunto $E$?

b) Indique quais são os pares ordenados que constituem a relação $R$ em $E$ assim definida:

$$xRy \Leftrightarrow x \text{ é paralela a } y$$

c) Quais são as propriedades que $R$ apresenta?

*Nota:* $x$ é paralela a $y$ quando $x = y$ ou $x \cap y = \emptyset$, com $x$ e $y$ coplanares.

**13.** Seja $E = \{1, 2, 3\}$. Considerem-se as seguintes relações em $E$:

$R_1 = \{(1, 1), (2, 2), (3, 3)\}$
$R_2 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$
$R_3 = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2), (3, 3)\}$
$R_4 = E \times E$
$R_5 = \emptyset$

Quais são reflexivas? E simétricas? E transitivas? E anti-simétricas?

**14.** Construa sobre o conjunto $E = \{1, 2, 3, 4\}$ quatro relações $R_1$, $R_2$, $R_3$ e $R_4$ de modo que $R_1$ só tem a propriedade reflexiva, $R_2$ só a simétrica, $R_3$ só a transitiva e $R_4$ só a anti-simétrica.

*Sugestão:* Faça os diagramas de flechas.

**15.** Dê um exemplo de relação $R$ sobre o conjunto $E = \{a, b, c\}$ que tenha as propriedades simétrica e anti-simétrica. Dê um exemplo de relação $S$ sobre $E$ que não tenha as propriedades simétrica e anti-simétrica.

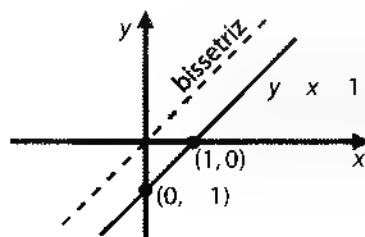
**16.** Descreva uma a uma todas as relações binárias sobre o conjunto $E = \{a, b\}$. Em seguida, identifique quais são reflexivas, quais são simétricas, quais são transitivas e quais são anti-simétricas.

### 1.9 Gráfico cartesiano e propriedades

Seja $R$ uma relação sobre o conjunto $\mathbb{R}$ dos números reais e seja $G_R$ seu gráfico cartesiano.

Quando $R$ é reflexiva, temos $(x, x) \in \mathbb{R}$ para todo $x$ real, ou seja, a reta bissetriz do 1º e 3º quadrantes do plano cartesiano é parte de $G_R$. E a recíproca também é válida.

*Exemplo 10.*

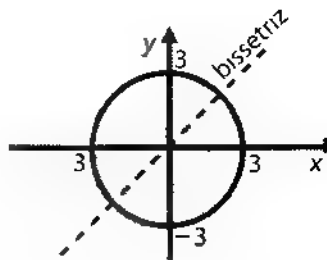
$R = \{(x, y) \in \mathbb{R}^2 \mid y \geqslant x - 1\}$ é reflexiva, pois $x \geqslant x - 1$, $\forall x$, ou seja, todo par $(x, x)$ está em $R$. A bissetriz está contida no gráfico de $R$ que é um semi-plano.

Quando $R$ é simétrica, se $(x, y) \in R$, então $(y, x) \in R$, ou seja, $G_R$ é simétrico relativamente à bissetriz do 1º e 3º quadrantes do plano cartesiano. E a recíproca também é válida.

*Exemplo 11:*

$R = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 9\}$ é simétrica, pois para todos $x$ e $y$ reais:

$$x^2 + y^2 \leq 9 \Rightarrow y^2 + x^2 \leq 9$$

Se o ponto $(x, y) \in R$, seu simétrico relativamente à bissetriz $(y, x) \in R$.

Dispomos, então, de mais um recurso para verificar se $R$ é reflexiva ou simétrica: observar seu gráfico cartesiano $G_R$.

## Exercícios

**17.** Esboce os gráficos cartesianos das seguintes relações sobre $\mathbb{R}$:

$R_1 = \{(x, y) \mid x + y \leq 2\}$

$R_2 = \{(x, y) \mid x^2 + y^2 = 1\}$

$R_3 = \{(x, y) \mid x^2 + y^2 \leq 4\}$

$R_4 = \{(x, y) \mid x^2 + x = y^2 + y\}$

$R_5 = \{(x, y) \mid x^2 + y^2 \geq 16\}$

**18.** Das relações do exercício anterior, quais são reflexivas? Quais são simétricas?

**19.** Esboce os gráficos cartesianos das seguintes relações sobre $\mathbb{R}$:

$R_6 = \{(x, y) \mid y = x^2\}$

$R_7 = \{(x, y) \mid xy = 12\}$

$R_8 = \{(x, y) \mid x^2 + 4y^2 \leq 4\}$

$R_9 = \{(x, y) \mid x^2 = y^2\}$

$R_{10} = \{(x, y) \mid y \geq x^3\}$

**20.** Das relações do exercício anterior, quais são reflexivas? Quais são simétricas?

## Exercícios complementares

**C1.** Seja $E$ um conjunto finito com $n$ elementos.

Quantas são as relações binárias sobre $E$?

Quantas dessas relações são reflexivas?

*Sugestão:* Use o fato de que uma relação $R$ sobre $E$ é reflexiva se, e somente se, $R = \Delta_E \cup R'$, em que $\Delta_E = \{(x, x) \mid x \in E\}$ e $R'$ é um subconjunto de $E \times E - \Delta_E$.

Quantas dessas relações são simétricas?

*Sugestão:* Use o fato de que uma relação $R$ sobre $E = \{a_1, a_2, a_3, ..., a_n\}$ é simétrica se, e somente se, $R = S \cup S^{-1}$, em que $S$ é um subconjunto de $E \times E$ constituído por pares da forma $(a_i, a_j)$, com $i \geq j$.

**C2.** Prove que, se uma relação $R$ é transitiva, então $R^{-1}$ também o é.

*Sugestão:* Tome $(x, y)$ e $(y, z)$ em $R^{-1}$ e mostre que $(x, z)$ está em $R^{-1}$.

**C3.** Sejam $R$ e $S$ relações no mesmo conjunto $E$. Prove que:

a) $R^{-1} \cap S^{-1} = (R \cap S)^{-1}$

b) $R^{-1} \cup S^{-1} = (R \cup S)^{-1}$

c) Se $R$ e $S$ são transitivas, então $R \cap S$ é transitiva.

d) Se $R$ e $S$ são simétricas, então $R \cup S$ e $R \cap S$ são simétricas

e) $R \cup R^{-1}$ é simétrica.

# 2. RELAÇÕES DE EQUIVALÊNCIA

## 2.1 Relação de equivalência

**Definição 11:** Uma relação $R$ sobre um conjunto $E$ não vazio é chamada *relação de equivalência* sobre $E$ se, e somente se, $R$ é reflexiva, simétrica e transitiva. Ou seja, $R$ deve cumprir, respectivamente, as seguintes propriedades:

(i) se $x \in E$, então $xRx$;

(ii) se $x, y \in E$ e $xRy$ então $yRx$;

(iii) se $x, y, z \in E$ e $xRy$ e $yRz$, então $xRz$.

*Exemplo 12:*

1º) A relação $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ sobre $E = \{a, b, c\}$ é uma relação de equivalência.

2º) A relação de igualdade sobre $\mathbb{R}$ é uma relação de equivalência, pois:

$(\forall x)\ (x \in \mathbb{R} \Rightarrow x = x)$

$(\forall x, y)\ (x = y \Rightarrow y = x)$

$(\forall x, y, z)\ (x = y \text{ e } y = z \Rightarrow x = z)$

3º) A relação de congruência módulo $m$ (em que $m \in \mathbb{Z}$ e $m > 1$) sobre $\mathbb{Z}$, definida no item 7 do capítulo 2, é uma relação de equivalência, pois:

$(\forall x)\ (x \in \mathbb{Z} \Rightarrow x \equiv x \pmod{m})$

$(\forall x, y)\ (x \equiv y \pmod{m} \Rightarrow y \equiv x \pmod{m})$

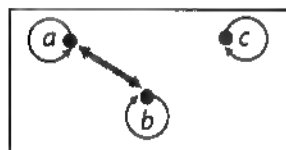
$(\forall x, y, z)\ (x \equiv y \pmod{m} \text{ e } y \equiv z \pmod{m} \Rightarrow x \equiv z \pmod{m})$

4º) A relação de paralelismo definida para as retas de um espaço $E$ euclidiano (ver exercício 12 deste capítulo) é uma relação de equivalência, pois, sendo $x$, $y$ e $z$ retas de $E$, tem-se:

(i) $(x \parallel x)$

(ii) $(x \parallel y \Rightarrow y \parallel x)$

(iii) $(x \parallel y \text{ e } y \parallel z \Rightarrow x \parallel z)$

### Exercícios

**21.** Quais das relações abaixo são relações de equivalência sobre $E = \{a, b, c\}$?

$R_1 = \{(a, a), (b, b), (c, c)\}$

$R_2 \quad \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\}$

$R_3 = \{(a, a), (b, b), (a, b), (b, a)\}$

$R_4 = E \times E$

$R_5 = \varnothing$

**22.** Quais das sentenças abertas abaixo definem uma relação de equivalência em $\mathbb{Z}$?

a) $x \equiv y \pmod 3$

b) $x \quad y$

c) $x \leqslant y$

d) $\text{mdc}(x, y) = 1$

e) $x + y = 7$

**23.** Seja $E$ o conjunto dos triângulos do espaço geométrico euclidiano. Seja $R$ a relação em $E$ definida por:

$$xRy \text{ se, e somente se, } x \text{ é semelhante a } y$$

Prove que $R$ é de equivalência.

**24.** Seja $E$ o conjunto das retas de um plano $\alpha$. Quais das relações abaixo definidas são relações de equivalência em $E$?

a) $xRy$ se, e somente se, $x \,//\, y$

b) $xSy$ se, e somente se, $x \perp y$

**25.** Considere a relação $R$ sobre $\mathbb{N} \times \mathbb{N}$ definida por:

$$(a, b)R(c, d) \text{ se, e somente se, } a + b = c + d$$

Prove que $R$ é uma relação de equivalência.

**26.** Pense na relação $S$ em $\mathbb{Z} \times \mathbb{Z}^*$ definida por:

$$(a, b)S(c, d) \text{ se, e somente se, } ad = bc$$

Prove que $S$ é uma relação de equivalência.

## 2.2 Classe de equivalência

**Definição 12:** Seja $R$ uma relação de equivalência sobre $E$. Dado $a$, com $a \in E$, chama-se *classe de equivalência* determinada por $a$, módulo $R$, o subconjunto de $a$ de $E$ constituído pelos elementos $x$ tais que $xRa$. Em símbolos:

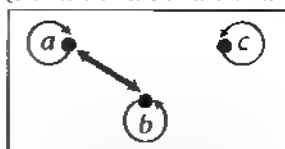
$$a \quad \{x \in E \mid xRa\}$$

## 2.3 Conjunto-quociente

**Definição 13:** O conjunto das classes de equivalência módulo $R$ será indicado por $E/R$ e chamado *conjunto-quociente* de $E$ por $R$.

*Exemplos 13:*

1º) Na relação de equivalência $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ temos:

$\bar{a} = \{a, b\}$
$\bar{b} = \{a, b\}$
$\bar{c} = \{c\}$
$E/R = \{\{a, b\}, \{c\}\}$

2º) A relação $R$ de congruência módulo $m$ ($m \in \mathbb{Z}$ e $m > 1$) sobre $\mathbb{Z}$ é uma relação de equivalência. Como é o conjunto-quociente $\mathbb{Z}/R$?

(i) Sendo $a \in \mathbb{Z}$, efetuemos a divisão euclidiana de $a$ por $m$, obtendo o quociente $q$ e o resto $r$. Temos

$$a = mq + r \quad \text{e} \quad 0 \leqslant r < m$$

e daí vem:

$$a - r = qm$$

Portanto:

$$a \equiv r \pmod{m}$$
$$\bar{a} = \bar{r}$$

Concluímos que $\bar{a}$ é uma classe igual a $\bar{r}$, em que $r$ é o resto da divisão de $a$ por $m$. Como $r \in \{0, 1, 2, ..., m - 1\}$, vem:

$$\bar{a} \in \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$$

(ii) Suponhamos que existam duas classes, $\bar{r}$ e $\bar{s}$, iguais em $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$, representadas por elementos $r$ e $s$, digamos $r < s$. Então:

$$\bar{r} = \bar{s} \text{ e } 0 \leqslant r < s < m$$

De $\bar{r} = \bar{s}$ segue que $r \equiv s \pmod{m}$ e, portanto, $m \mid s - r$; como $0 < s - r < m$, isso é impossível.

Concluímos que $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$ é constituído por exatamente $m$ elementos distintos dois a dois, ou seja:

$$\mathbb{Z}/R = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$$

**Proposição 1:** Seja $R$ uma relação de equivalência sobre $E$ e sejam $a \in E$ e $b \in E$. As seguintes proposições são equivalentes:

(I) $aRb$ (II) $a \in \bar{b}$ (III) $b \in \bar{a}$ (IV) $\bar{a} = \bar{b}$

*Demonstração:* Devemos provar que (I) $\Rightarrow$ (II) $\Rightarrow$ (III) $\Rightarrow$ (IV) $\Rightarrow$ (I).

(I) $\Rightarrow$ (II): É decorrência de definição de classe de equivalência

(II) $\Rightarrow$ (III): Como $a \in \bar{b}$, então $aRb$. Daí, pela simetria de $R$, $bRa$ e, portanto, $b \in \bar{a}$.

(III) $\Rightarrow$ (IV) Por hipotese, $b \in \bar{a}$, ou seja, $bRa$. Logo, $aRb$ Temos de provar que $\bar{a} \subset \bar{b}$ e $\bar{b} \subset \bar{a}$.

Para provar a primeira dessas inclusões, tomemos $x \in \bar{a}$ Então, $xRa$ e, levando em conta que $aRb$, concluímos, pela transitividade de $R$, que $xRb$. Daí $x \in \bar{b}$ e, entao, $\bar{a} \subset \bar{b}$.

Analogamente se prova que $\bar{b} \subset \bar{a}$.

(IV) $\rightarrow$ (I): Como $a \in \bar{a}$ e $b \in \bar{b}$, os conjuntos $\bar{a}$ e $\bar{b}$ nao sao vazios. Tomemos um $x \in \bar{a} \cap \bar{b}$. Então, $xRa$ e $xRb$. Daí, pela simetria de $R$, valem $aRx$ e $xRb$. A transitividade de $R$ garante, então, que $aRb$. #

## Exercícios

**27.** Seja $E = \{x \in \mathbb{Z} \mid -5 \leqslant x \leqslant 5\}$ e seja $R$ a relação sobre $E$ definida por

$$xRy \text{ se, e somente se, } x^2 + 2x = y^2 + 2y$$

a) Mostre que $R$ é uma relação de equivalência.

b) Descreva as classes de equivalência $\overline{0}$, $\overline{-2}$, e $\overline{4}$.

**28.** Sejam $E = \{x \in \mathbb{Z} \mid |x| \leqslant 3\}$ e $R$ a relação sobre $E$ definida por

$$xRy \text{ se, e somente se, } x + |x| = y + |y|$$

a) Mostre que $R$ é uma relação de equivalência.

b) Descreva o conjunto-quociente $E/R$.

**29.** Considere o conjunto $E = \{x \in \mathbb{Z} \mid 0 \leqslant x \leqslant 10\}$ e sobre ele a relação $R$ de congruência módulo 4, que é de equivalência.

a) Descreva as classes de equivalência $\overline{0}$ e $\overline{1}$.

b) Descreva o conjunto-quociente $E/R$.

**30.** Seja $R$ a relação sobre $\mathbb{Q}$ definida da seguinte forma:

$$xRy \text{ se, e somente se, } x - y \in \mathbb{Z}$$

a) Prove que $R$ é uma relação de equivalência.

b) Descreva a classe $\overline{100}$.

c) Descreva a classe $\overline{0{,}5}$.

**31.** Considere a relação $S$ sobre $\mathbb{R}$ definida da seguinte forma:

$$xSy \text{ se, e somente se, } x - y \in \mathbb{Q}$$

a) Prove que $S$ é uma relação de equivalência.

b) Descreva a classe representada por $\frac{1}{2}$.

c) Descreva a classe $\bar{a}$, quando $a \in \mathbb{Q}$.

d) Descreva a classe $\overline{\sqrt{2}}$.

**32.** Pense na relação $T$ sobre $\mathbb{C}$ definida por

$$(x + yi)\,T\,(z + ti) \text{ se, e somente se, } x^2 + y^2 \quad z^2 + t^2$$

com $x, y, z$ e $t$ reais.

a) Prove que $T$ é uma relação de equivalência.

b) Descreva a classe $1 + i$.

**33.** Mostre que a relação $R \quad \{(a + bi, c + di) \mid b \quad d\}$ é uma relaçao de equivalên cia sobre $\mathbb{C}$ e descreva o conjunto-quociente $\mathbb{C}/R$.

**34.** Mostre que a relação $S$ sobre $\mathbb{R}^2$ definida por

$$(x_1, y_1)\,S\,(x_2, y_2) \text{ se, e somente se, } x_1 y_1 = x_2 y_2$$

é uma relação de equivalência. A seguir descreva as classes $\overline{(0, 0)}$ e $\overline{(1, 1)}$. Finalmente descreva $\mathbb{R}^2/S$.

**35.** Mostre que a relação $T$ sobre $\mathbb{R}^2$ definida por

$$(x_1, y_1)\,T\,(x_2, y_2) \text{ se, e somente se, } x_1 - y_1 = x_2 - y_2$$

é uma relação de equivalência. A seguir descreva $\overline{(1, 1)}$, $\overline{(1, 3)}$ e $\mathbb{R}^2 / T$.

## 2.4 Partição de um conjunto

**Definição 14:** Seja $E$ um conjunto não vazio. Diz-se que uma classe $\mathcal{F}$ de subconjuntos não vazios de $E$ é uma *partição* de $E$ se, e somente se:

a) dois membros quaisquer de $\mathcal{F}$ ou são iguais ou são disjuntos;

b) a união dos membros de $\mathcal{F}$ é igual a $E$.

*Exemplos 14:*

1º) $\mathcal{F} = \{\{1\}, \{2, 3\}, \{4\}\}$ é uma partição do conjunto $E = \{1, 2, 3, 4\}$.

2º) Sejam:

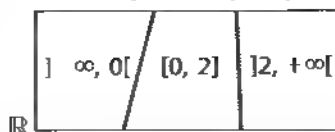
$P = \{x \in \mathbb{Z} \mid x \text{ é par}\}$

$I = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$

então $\mathcal{F} = \{P, I\}$ é uma partição de $\mathbb{Z}$.

3º) $\mathscr{F} = \{]-\infty, 0[, [0, 2], ]2, +\infty[\}$ é uma partição de $\mathbb{R}$

| $]-\infty, 0[$ | $[0, 2]$ | $]2, +\infty[$ |
|---|---|---|

$\mathbb{R}$

Provaremos que, através de uma relação de equivalência sobre o conjunto $E$, fica determinada uma partição de $E$ (proposição 2). Em seguida, provaremos a recíproca, ou seja, que a cada partição de $E$ pode ser associada uma relação de equivalência sobre $E$ (proposição 3).

Certos conceitos matemáticos, como os de número inteiro, número racional, número real, vetor, etc., são fixados no plano formal através de relações de equivalência e classes de equivalência cuja construção se baseia nos teoremas a seguir.

**Proposição 2:** Se $R$ é uma relação de equivalência sobre um conjunto $E$, então $E/R$ é uma partição de $E$.

*Demonstração:*

a) Seja $\bar{a} \in E/R$. Como $R$ é reflexiva, $aRa$ e, portanto, $a \in \bar{a}$. Assim, $\bar{a} \neq \varnothing$ para todo $\bar{a} \in E/R$.

b) Sejam $\bar{a} \in E/R$ e $\bar{b} \in E/R$ tais que $\bar{a} \cap \bar{b} \neq \varnothing$. Provaremos que $\bar{a} = \bar{b}$.

De fato, seja $y \in \bar{a} \cap \bar{b}$. Então, $y \in \bar{a}$ e $y \in \bar{b}$ e, portanto, $yRa$ e $yRb$. Daí, $aRy$ e $yRb$ e, portanto, $aRb$. A proposição 1 garante, então, que $\bar{a} = \bar{b}$.

c) Provemos que $\bigcup_{a \in E} \bar{a} = E$.

(i) Para cada $a \in E$, temos $\bar{a} \subset E$; portanto, $\bigcup_{a \in E} \bar{a} \subset E$.

(ii) Sendo $x$ um elemento qualquer de $E$, então $xRx$. Daí, $x \in \bar{x}$ e, por conseguinte, $x \in \bigcup_{a \in E} \bar{a}$.

Assim, $E \subset \bigcup_{a \in E} \bar{a}$. #

**Proposição 3:** Se $\mathscr{F}$ é uma partição do conjunto $E$, então existe uma relação $R$ de equivalência sobre $E$ tal que $E/R = \mathscr{F}$.

*Demonstração:* Seja $R$ a relação sobre $E$ assim definida: $xRy$ se, e somente se, $\exists A \in \mathscr{F}$ tal que $x \in A$ e $y \in A$, ou seja, $x$ está relacionado com $y$ quando existe um conjunto $A$ da partição $\mathscr{F}$ ao qual pertencem $x$ e $y$. Provaremos que $R$ é relação de equivalência.

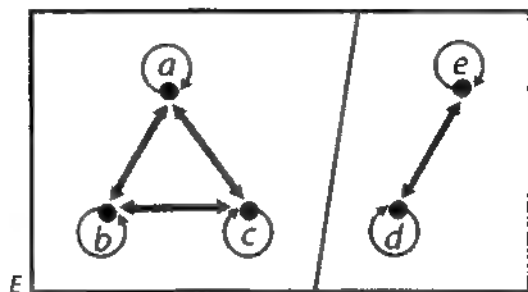
Temos

(i) Para todo $x$ em $E$ existe um subconjunto $A \subset E$ tal que $A \in \mathscr{F}$ e $x \in A$; portanto $xRx$

(ii) Se $x$ e $y$ são elementos quaisquer de $E$ tais que $xRy$, então $x, y \in A$, para algum $A \in \mathscr{F}$. Obviamente, então, $y, x \in A$. Logo $yRx$. #

(iii) Sejam $x$, $y$ e $z$ elementos quaisquer de $E$ tais que $xRy$ e $yRz$. Isso significa que $x, y \in A$ e $y, z \in B$, para convenientes $A, B \in \mathcal{F}$. Logo, $y \in A$ e $y \in B$ Como dois conjuntos quaisquer de $\mathcal{F}$ que não são disjuntos são necessariamente iguais, então $A$ $B$ Desse fato decorre que $x$ e $z$ pertencem ao mesmo conjunto da classe $\mathcal{F}$. De onde, $x R z$.

*Exemplo 15:* Dada a partição $\mathcal{F} = \{\{a, b, c\}, \{d, e\}\}$ de $E - \{a, b, c, d, e\}$, a ela podemos associar a relação de equivalência $R$ $\{(a, a), (a, b), (b, a), (b, b), (b, c), (c, b), (c, c), (a, c), (c, a), (d, d), (d, e), (e, d), (e, e)\}$.

Observar que $E/R = \{\{a, b, c\}, \{d, e\}\} = \mathcal{F}$.

## Exercícios

**36.** Qual é a relação de equivalência associada a cada uma das seguintes partições?

a) $\mathcal{F}_1 = \{\{a, b\}, (c, d)\}$

b) $\mathcal{F}_2 = \{\{a\}, \{b\}, \{c, d\}\}$

c) $\mathcal{F}_3 = \{\{0, \pm 2, \pm 4, \ldots\}, \{\pm 1, \pm 3, \pm 5, \ldots\}\}$

**37.** Quais são as relações de equivalência sobre $E = \{a, b\}$?

**38.** Descreva uma a uma todas as relações de equivalência sobre $E = \{a, b, c\}$.

**39.** Quantas são as relações de equivalência que podem ser estabelecidas sobre um conjunto de 4 elementos?

## Exercícios complementares

**C4.** Seja $E$ o conjunto das retas de um plano $\alpha$ e seja $P$ um ponto fixado de $\alpha$ Considere a relação $R$ em $E$ assim definida:

$$xRy \text{ se, e somente se, } P \in x \cap y$$

$R$ é uma relação de equivalência?

**C5.** Seja $E$ um conjunto não vazio Dados $X, Y \in \mathscr{P}(E)$, mostre que as relações $R$ e $S$ abaixo definidas são de equivalência em $\mathscr{P}(E)$.

a) $XRY$ se, e somente se, $X \cap A = Y \cap A$

b) $XSY$ se, e somente se, $X \cup A = Y \cup A$

em que $A$ é um subconjunto fixado de $E$.

**C6.** Seja $R$ uma relação reflexiva sobre $E$ com as seguintes propriedades:

1) $D(R) = E$

2) $(\forall a, b, c \in E)$(se $aRc$ e $bRc$, então $aRb$)

Mostre que $R$ é uma relação de equivalência.

**C7.** Seja $R$ a relação sobre $\mathbb{Z}$ assim definida:

$$xRy \text{ se, e somente se, } x \mid y \text{ e } y \mid x$$

Mostre que $R$ é uma relação de equivalência e descreva o conjunto-quociente $\mathbb{Z}/R$.

**C8.** Seja $S$ a relação definida em $\mathbb{R}^2$ da seguinte forma.

$$(x_1, y_1)S(x_2, y_2) \text{ se, e somente se, } 4x_1^2 + 9y_1^2 = 4x_2^2 + 9y_2^2$$

a) Prove que $S$ é uma relaçao de equivalência.

b) Descreva geometricamente a classe $\overline{(3, 0)}$.

c) Descreva o conjunto-quociente $\mathbb{R}^2/S$.

# 3. RELAÇÕES DE ORDEM

## 3.1 Relação de ordem. Conjuntos ordenados

**Definição 15:** Uma relação $R$ sobre um conjunto $E$ não vazio é chamada *relação de ordem parcial* sobre $E$ se, e somente se, $R$ é reflexiva anti-simétrica e transitiva. Ou seja, $R$ deve cumprir respectivamente as seguintes propriedades:

(i) Se $x \in E$, então $xRx$;

(ii) Se $x, y \in E$, $xRy$ e $yRx$, então $x = y$;

(iii) Se $x, y, z \in E$, $xRy$ e $yRz$, então $xRz$.

Quando $R$ é uma relação de ordem parcial sobre $E$, para exprimir que $(a, b) \in R$, usaremos a notação $a \preccurlyeq b$ $(R)$, que se lê "$a$ precede $b$ na relação $R$" ou "$b$ segue $a$ na relação $R$". Para exprimir que $(a, b) \in R$ e $a \neq b$, usaremos a notação $a < b$ $(R)$, que se lê "$a$ precede estritamente $b$ na relação $R$" ou "$b$ segue estritamente $a$ na relação $R$".

Outra notaçao que se poderá usar para exprimir que "$a$ precede $b$" é "$a \preccurlyeq b$" Mas isso pressupõe o entendimento de que, nesse caso, "$\preccurlyeq$" não significa necessariamen

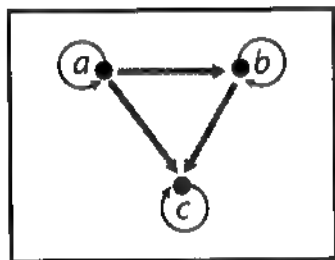
te "menor ou igual a", no sentido numérico usual. O sentido é aquele definido pelo contexto da questao em foco. Analogamente, a notação "$a < b$" poderá ser usada para exprimir que "$a$ precede estritamente $b$", com um sentido que não o usual.

**Definição 16:** Um *conjunto parcialmente ordenado* é um conjunto sobre o qual se definiu uma certa relação de ordem parcial.

**Definição 17:** Seja $R$ uma relação de ordem parcial sobre $E$ Os elementos $a$, $b \in E$ se dizem *comparáveis mediante* R se $a \preccurlyeq b$ ou $b \preccurlyeq a$.

**Definição 18:** Se dois elementos quaisquer de $E$ forem comparáveis mediante $R$, então $R$ sera chamada relação de ordem total sobre $E$. Nesse caso, o conjunto $E$ é dito *conjunto totalmente ordenado* por $R$.

*Exemplos 16:*

1º) A relação $R = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\}$ é uma relação de ordem sobre $E = \{a, b, c\}$, conforme se pode notar no diagrama ao lado. O conjunto $E$ é totalmente ordenado por $R$, uma vez que não há dois pontos distintos de $E$ que não estejam ligados por uma flecha.

2º) A relação $R$ sobre $\mathbb{R}$ definida por

$$x\,R\,y \text{ se, e somente se, } x \leqslant y \quad (\leqslant: \text{"menor ou igual a"})$$

é uma relação de ordem, denominada ordem habitual, pois:

$(\forall x)\ (x \in \mathbb{R} \Rightarrow x \leqslant x)$

$(\forall x, y \in \mathbb{R})\ (x \leqslant y \text{ e } y \leqslant x \Rightarrow x = y)$

$(\forall x, y, z \in \mathbb{R})\ (x \leqslant y \text{ e } y \leqslant z \Rightarrow x \leqslant z)$

O conjunto $\mathbb{R}$ é totalmente ordenado pela relação de ordem habitual, pois se $x, y \in \mathbb{R}$, então $x \leqslant y$ ou $y \leqslant x$.

3º) A relação $R$ sobre $\mathbb{N}$ definida por

$$xRy \text{ se, e somente se, } x \mid y \quad (|: \text{"é divisor de"})$$

é uma relação de ordem, pois:

$(\forall x)\ (x \in \mathbb{N} \Rightarrow x \mid x)$

$(\forall x, y \in \mathbb{N})\ (x \mid y \text{ e } y \mid x \Rightarrow x = y)$

$(\forall x, y, z \in \mathbb{N})\ (x \mid y \text{ e } y \mid z \Rightarrow x \mid z)$

como se pode provar facilmente usando-se o conceito de divisor visto no **cap. II. 3.**

O conjunto $\mathbb{N}$ é parcialmente ordenado por essa relaçao Essa ordem não ordena totalmente $\mathbb{N}$ porque há elementos de $\mathbb{N}$ não comparáveis por divisibilidade, como, por exemplo, o 2 e o 3·

$$2 \nmid 3 \quad \text{e} \quad 3 \nmid 2$$

4º) A relação de inclusão sobre uma família $\mathcal{F}$ de subconjuntos de um dado conjunto $E$ é uma relação de ordem, pois:

$(\forall x)\ (x \in \mathcal{F} \Rightarrow x \subset x)$

$(\forall x, y \in \mathcal{F})\ (x \subset y \text{ e } y \subset x \Rightarrow x = y)$

$(\forall x, y, z \in \mathcal{F})\ (x \subset y \text{ e } y \subset z \Rightarrow x \subset z)$

## Exercícios

**40.** Seja $\mathbb{C}$ o conjunto dos números complexos e sejam $x = a + bi$ e $y = c + di$ dois elementos de $\mathbb{C}$. Considere a relação $R$ sobre $\mathbb{C}$ definida por:

$$xRy \text{ se, e somente se, } a \leqslant c \text{ e } b \leqslant d$$

a) Mostre que $R$ é uma relação de ordem parcial sobre $\mathbb{C}$.

b) Assinale no plano de Argand-Gauss o conjunto $A$ dos complexos $z$ tais que $zR(1 + 2i)$ e o conjunto $B$ dos complexos $z$ tais que $(1 + 2i)Rz$.

c) Decida: $\mathbb{C}$ é totalmente ordenado por $R$?

**41.** Prove que, se $R$ é uma relação de ordem parcial sobre $E$, então $R^{-1}$ também é.
*Nota:* Nesse caso, $R^{-1}$ é denominada *ordem oposta* de $R$.

**42.** Seja $\mathbb{C}$ o conjunto dos números complexos e sejam $x = a + bi$ e $y = c + di$ dois elementos de $\mathbb{C}$. Considere a relação $S$ sobre $\mathbb{C}$ assim definida:

$$xSy \text{ se, e somente se, } a < c \text{ ou } (a = c \text{ e } b \leqslant d)$$

a) Mostre que $S$ é uma relação de ordem parcial sobre $\mathbb{C}$.

b) Assinale no plano de Argand-Gauss o conjunto $A$ dos complexos $z$ tais que $zS(1 + 2i)$ e o conjunto $B$ dos complexos z tais que $(1 + 2i)Sz$.

c) Decida: $\mathbb{C}$ é totalmente ordenado por $S$?

**43.** Prove que a relação $S$ sobre $\mathbb{N} \times \mathbb{N}$ tal que $(a, b)S(c, d)$ se, e somente se, $a \mid c$ e $b \mid d$ é uma relação de ordem. A relação $S$ ordena totalmente $\mathbb{N} \times \mathbb{N}$?

## 3.2 Representação gráfica simplificada

Para representar uma relação de ordem sobre um conjunto finito $E$, podemos utilizar um esquema simplificado que substitui o esquema de flechas já visto. É assim:

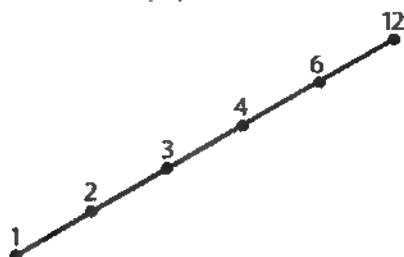
1º) quando $aRb$, ligamos o elemento $a$ ao elemento $b$ por meio de um traço ascendente,

2º) deixamos de desenhar os laços em torno de cada elemento de $E$ (não expomos a propriedade reflexiva);

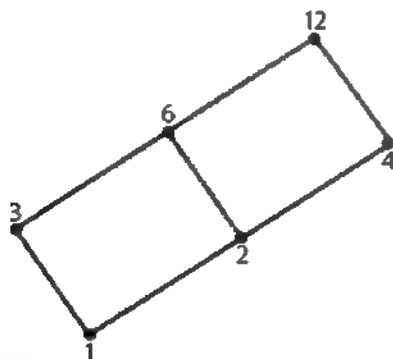
3°) quando existe um traço ligando *a* com *b* e um outro traço ligando *b* com *c*, deixamos de desenhar um traço ligando *a* com *c* (não expomos a propriedade transitiva).

*Exemplos 17:*

1º) $E = \{1, 2, 3, 4, 6, 12\}$

*R* é a ordem habitual ($\leq$).

*E* é totalmente ordenado por *R*.

2º) $E = \{1, 2, 3, 4, 6, 12\}$

*S* é a ordem por divisibilidade.

*E* é parcialmente ordenado por *S*.

## Exercícios

**44.** Faça o diagrama simplificado das seguintes ordens no conjunto $E = \{1, 2, 4, 5, 10, 20\}$:

a) ordem habitual;

b) ordem por divisibilidade.

**45.** Faça o diagrama simplificado da relação de ordem por inclusão em $E = \mathcal{P}(\{a, b\})$.

**46.** Faça o diagrama simplificado da relação de ordem por divisibilidade no conjunto $E = \{2, 3, 5, 6, 10, 15, 30\}$.

**47.** Faça o diagrama simplificado da relação de ordem por inclusão no conjunto $E = \{\{a\}, \{b\}, \{a, b, c\}, \{a, b, d\}, \{a, b, c, d\}, \{a, b, c, d, e\}\}$.

## 3.3 Limites superiores e inferiores

Seja $E$ um conjunto parcialmente ordenado mediante a relação $\leqslant$. Seja $A$ um subconjunto de $E$, com $A \neq \varnothing$.

**Definição 19:** Um elemento $L \in E$ é um *limite superior* de $A$ se, para todo $x \in A$, valer $x \leqslant L$, isto é, qualquer elemento de $A$ precede $L$.

**Definição 20:** Um elemento $\ell \in E$ é um *limite inferior* de $A$ se, para todo $x \in A$, valer $\ell \leqslant x$, isto e, $\ell$ precede qualquer elemento de $A$.

## 3.4 Máximo e mínimo

Seja $A$ um subconjunto não vazio do conjunto $E$ parcialmente ordenado pela relação $\leqslant$.

**Definição 21:** Um elemento $M \in A$ é um *máximo* de $A$ se, para todo $x \in A$, valer $x \leqslant M$, isto é se $M$ é um limite superior de $A$ e pertence a $A$.

**Definição 22:** Um elemento $m \in A$ é um *mínimo* de $A$ se, para todo $x \in A$, valer $m \leqslant x$, isto é, se $m$ é um limite inferior de $A$ e pertence a $A$.

**Proposição 4:** Se $A$ é um subconjunto do conjunto parcialmente ordenado $E$ e existe um máximo (ou mínimo) de $A$, então ele é único.

*Demonstração:* Admitamos que $M_1$ e $M_2$ sejam máximos de $A$. Como $M_1$ é máximo de $A$ e $M_2 \in A$, então $M_2 \leqslant M_1$. Por raciocínio análogo, prova-se que $M_1 \leqslant M_2$. Logo, $M_1 = M_2$.

Para o mínimo, a demonstração é semelhante. #

## 3.5 Supremo e ínfimo

**Definição 23:** Seja $A$ um subconjunto não vazio do conjunto parcialmente ordenado $E$. Chama-se *supremo* de $A$ o mínimo, caso exista, do conjunto dos limites superiores de $A$. Chama-se *ínfimo* de $A$ o máximo, caso exista, do conjunto dos limites inferiores de $A$.

## 3.6 Elementos maximais e minimais

Seja $A$ um subconjunto nao vazio do conjunto parcialmente ordenado $E$.

**Definição 24:** Um elemento $m_1 \in A$ é um *elemento maximal* de $A$ se nenhum elemento de $A$ segue estritamente $m_1$. Em outras palavras: se $x \in A$ e $m_1 \leqslant x$, então $m_1 = x$.

**Definição 25:** Um elemento $m_0 \in A$ é um *elemento minimal* de $A$ se nenhum elemento de $A$ precede estritamente $m_0$. Em outras palavras: se $x \in A$ e $x \preceq m_0$, então $m_0 = x$.

*Exemplos 18:*

1°) Se $E = \mathbb{R}$, $A = \{x \in \mathbb{R} \mid 0 < x \leq 1\} = ]0, 1]$ e a ordem é a habitual, temos:

a) são limites superiores de $A$ os números reais $L \geq 1$;

b) são limites inferiores de $A$ os números reais $\ell \leq 0$;

c) o máximo de $A$ é 1;

d) $A$ não possui mínimo;

e) o supremo de $A$ é 1;

f) o ínfimo de $A$ é 0;

g) 1 é o único elemento maximal de $A$;

h) $A$ não tem elementos minimais.

2º) Se $E = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $A = \{2, 4, 6\}$ e a ordem é a divisibilidade, o diagrama simplificado abaixo mostra que:

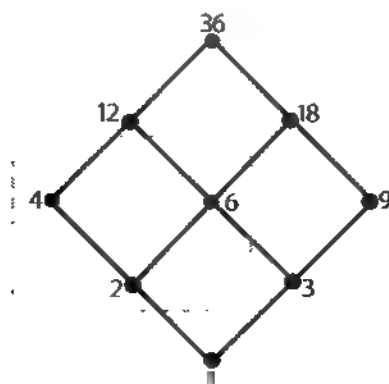
a) os limites superiores de $A$ são 12 e 36;

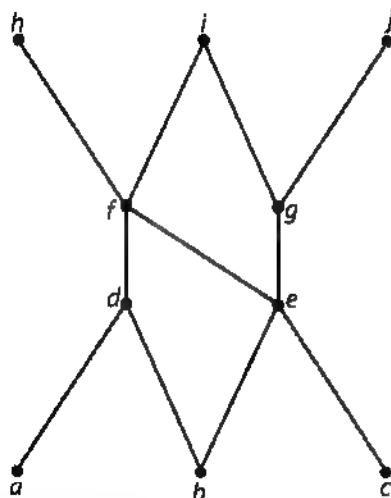
b) os limites inferiores de $A$ são 1 e 2;

c) $A$ tem mínimo 2 e não tem máximo;

d) $A$ tem ínfimo 2 e supremo 12;

e) só 2 é elemento minimal de $A$;

f) os elementos maximais de $A$ são 4 e 6.

## Exercícios

**48.** O diagrama abaixo representa uma relação de ordem $R$ sobre $E = \{a, b, c, d, e, f, g, h, i, j\}$.

Determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo e o mínimo de $A = \{d, e\}$.

**49.** Seja $A = \{x \in \mathbb{Q} \mid 0 < x^2 < 2\}$ um subconjunto de $\mathbb{Q}$, em que se considera a relação de ordem habitual. Determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo e o mínimo de $A$

**50.** Utilize o resultado do exercício 46 e determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo e o mínimo de $A = \{6, 10\}$.

**51.** Utilize o resultado do exercício 47 e determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo e o mínimo de $A = \{\{a, b, c\}, \{a, b, d\}, \{a, b, c, d\}\}$.

**52.** Considere a relação $R$ definida em $\mathbb{N} \times \mathbb{N}$ da seguinte forma:

$$(a, b) R (c, d) \text{ se, e somente se, } a \mid c \text{ e } b \leqslant d$$

(i) Prove que $R$ é uma relação de ordem parcial.

(ii) Determine os limites superiores, os limites inferiores, o supremo, o ínfimo, o máximo e o mínimo de $A = \{(1, 2), (2, 1)\}$.

### Exercícios complementares

**C9.** Sejam $E$ e $F$ dois conjuntos totalmente ordenados pela relação $\leqslant$. Sejam $\alpha = (x, y)$ e $\beta = (x', y')$ elementos de $E \times F$, em que está definida a relação $R$ da forma seguinte:

$$\alpha R \beta \text{ se, e somente se, } (x \leqslant x' \text{ ou } (x = x' \text{ e } y \leqslant y'))$$

Prove que $R$ é uma relação de ordem total em $E \times F$.

**C10.** Faça um diagrama simplificado da relação de inclusão sobre $\mathcal{P}(E)$ em que $E = \{a, b, c\}$, com $a \neq b \neq c \neq a$.

# III-2 APLICAÇÕES

## 4. NOTA HISTÓRICA (A FORMAÇÃO DO CONCEITO DE FUNÇÃO)

Só no século XIX, a idéia de função ganharia forma matemática. Mas desde a Antiguidade ela aparece embrionariamente, como, por exemplo, entre os babilônios. Efetivamente, os babilônios foram exímios produtores de tábuas matemáticas. Uma das remanescentes traz os valores de $n^3 + n^2$, para $n = 1, 2, 3, ..., 20, 30, 40$ e $50$. Obviamente, não seria forçado associá-la à função $f$ cujo domínio é $\{1, 2, 3, ..., 29, 30, 40, 50\}$ e que está definida por $f(x) = x^3 + x^2$. Mas, como possivelmente essa tábua foi construída para permitir a resolução de equações do tipo $x^3 + x^2 = c$, pode-se ver nela ainda o germe da idéia de função inversa. De fato, ao se resolver a equação $x^3 + x^2 = 80$, por exemplo, o que se procura é o número $n$ tal que $f(n) = 80$, ou seja, a "imagem" de 80 pela "função inversa" de $f$.

Em sua obra-prima, *O almagesto*, Claúdio Ptolomeu (século II d.C.) deu um grande passo nessa matéria. Em seu livro I (são 13 ao todo) há uma tábua com as cordas dos arcos de 1/2° a 180° em intervalos de 1/2°. Essas cordas são, na verdade, os ancestrais mais remotos de nossos senos. Como Ptolomeu usou também suas tábuas em sentido contrário, para achar, por exemplo, o arco de uma dada corda, é plausível dizer que a idéia de função inversa também está presente em sua obra. Mas o grande passo de Ptolomeu consistiu em mostrar como interpolar linhas em sua tábua, para qualquer valor da "variável independente" (o arco), o que sugeria um caminho para um estudo computacional de fenômenos contínuos

No período medieval não se verificaram avanços significativos na formação do conceito de funçao. De um lado porque a álgebra literal, fundamental para explorar esse conceito, só seria criada no final do século XVI. De outro, porque a ciência ainda nao elegera a descrição quantitativa dos fenômenos como meta, o que só aconteceria no Renascimento, graças principalmente a Galileu Galilei (1564-1642). Portanto, não sem motivos, há historiadores que atribuem a esse sábio a criação do conceito de função.

Galileu aplicou seu método científico principalmente ao estudo do movimento. Por exemplo, em *Diálogos sobre duas novas ciências* (1638), encontra se a seguinte le "Os espaços percorridos por um corpo que sai do repouso em movimento uniformemente acelerado estão entre si como os quadrados dos tempos gastos para percorrê-los". Ou seja, se para percorrer determinado espaço $s_1$ o tempo gasto é $t_1$ e se para percorrer um espaço $s$ o tempo gasto é $t$, então $\frac{s}{s_1} = \frac{t^2}{t_1^2}$. Com o desenvolvimento e a difusão da simbologia algébrica (ignorada por Galileu), essa lei passaria a se escrever assim:

$$s = kt^2$$

em que $k = s_1/t_1^2$, destacando-se o espaço em termos do tempo.

Mas quem primeiro conseguiu fundir à idéia de variabilidade uma simbologia algébrica conveniente, ao representar lugares geométricos por meio de equações algébricas e fazer a correspondência entre as variáveis a fim de poder esboçar o gráfico correspondente, foi o filósofo e matemático francês René Descartes (1596-1650), o criador da geometria analítica.

Na segunda metade do século XVII, o matemático alemão G W. Leibniz (1646-1716) usaria pela primeira vez a palavra "funçao". Também se deve a Leibniz a introdução das palavras "variável", "constante" e "parâmetro", hoje corriqueiras na linguagem matemática. Mas a notação $f(x)$ para indicar uma função só seria introduzida em 1734 pelo matemático suíço L. Euler (1707 1783).

## 5. APLICAÇÃO — FUNÇÃO

**Definição 26:** Seja $f$ uma relação de $E$ em $F$. Dizemos que $f$ é uma *aplicação* de $E$ em $F$ se, e somente se:

(i) o domínio de $f$ é $E$, isto é, $D(f) = E$;

(ii) dado um elemento $a \in D(f)$, é único o elemento $b \in F$ tal que $(a, b) \in f$.

Se $f$ é uma aplicação de $E$ em $F$, escrevemos:

$$b = f(a) \text{ (lê-se "} b \text{ é imagem de } a \text{ pela } f\text{")}$$

para indicar que $(a, b) \in f$.

Usaremos também a notação

$$f: E \to F$$

para indicar que $f$ é uma aplicação de $E$ em $F$.

Às vezes, usaremos a notação

$$x \mapsto f(x)$$

para indicar a aplicação $f$ em que $f(x)$ é a imagem do elemento genérico $x$.

O conjunto $F$ é chamado contradomínio de $f$.

*Igualdade.* decorre diretamente da definição de relação (seção **1.2** deste capítulo) a seguinte proposição: se $f: E \to F$ e $g: E \to F$, então $f = g$ se $f(x) = g(x)$ para todo $x \in E$.

*Função.* se $f. E \to F$ e o contradomínio $F$ é um conjunto numérico (portanto, $F$ é subconjunto de $\mathbb{C}$), é usual chamar $f$ de função. Às vezes, contudo, usa se a palavra função para designar uma aplicação qualquer.

*Exemplos 19 e contra exemplos 5:*

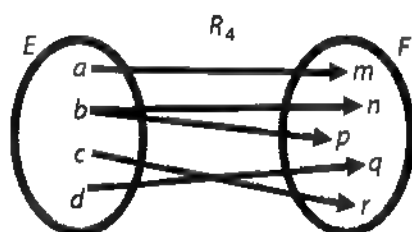
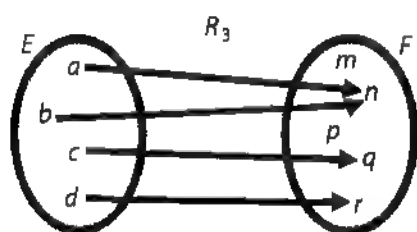
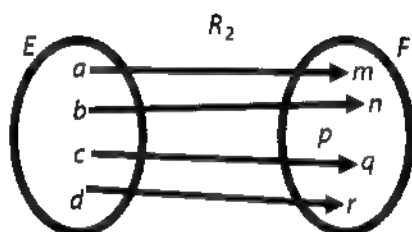
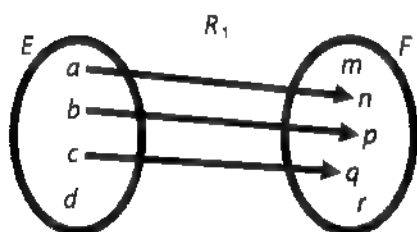
1º) Se $E = \{a, b, c, d\}$ e $F = \{m, n, p, q, r\}$, consideremos as relações de $E$ em $F$ seguintes.

$R_1 = \{(a, n), (b, p), (c, q)\}$

$R_2 = \{(a, m), (b, n), (c, q), (d, r)\}$

$R_3 = \{(a, n), (b, n), (c, q), (d, r)\}$

$R_4 = \{(a, m), (b, n), (b, p), (c, r), (d, q)\}$

Examinemos os diagramas de flechas:

Temos:

$R_2$ e $R_3$ são aplicações;

$R_1$ não é aplicação, pois $D(R_1) = \{a, b, c\} \neq E$, uma vez que $d \notin D(R_1)$;

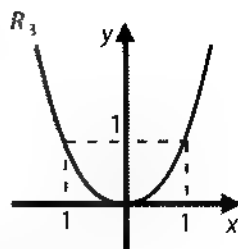
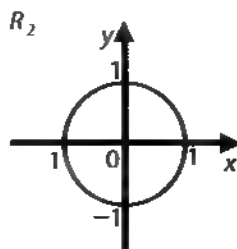
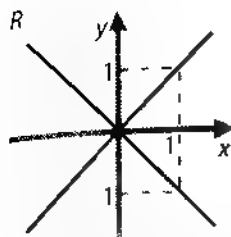
$R_4$ não é aplicação, pois $(b, n) \in R_4$ e $(b, p) \in R_4$, portanto, $b$ tem dois "correspondentes" em $F$

2º) Se $E = F = \mathbb{R}$, consideremos as seguintes relações de $\mathbb{R}$ em $\mathbb{R}$:

$R_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 = y^2\}$

$R_2 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$

$R_3 = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$

Examinemos seus gráficos cartesianos:

A relação $R_1$ não é aplicação, pois, por exemplo, para $a = 1$ existem $b = 1$ e $b' = -1$ tais que $(a, b)$ e $(a, b')$ estão em $R_1$.

A relação $R_2$ não é aplicação, pois $D(R_2) = [-1, 1] \neq \mathbb{R}$ e também porque, por exemplo, para $a = 0$ existem $b = 1$ e $b' = -1$ tais que $(a, b) \in R_2$ e $(a, b') \in R_2$.

A relação $R_3$ é aplicação de $\mathbb{R}$ em $\mathbb{R}$.

## Exercícios

**53.** Se $E = \{1, 2, 3, 4\}$ e $F = \{a, b, c\}$, quais das relações abaixo são aplicações de $E$ em $F$?

$R_1 = \{(1, a), (2, b), (3, c)\}$
$R_2 = \{(1, a), (2, b), (3, c), (4, c)\}$
$R_3 = \{(1, b), (1, c), (2, b), (3, c), (4, a)\}$
$R_4 = \{(1, c), (2, c), (3, c), (4, c)\}$

**54.** Considere a relação $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 9\}$. $R$ é uma aplicação?

**55.** Considere a relação $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid mx + ny = 1\}$, em que $m$ e $n$ são números inteiros dados. Quais são as condições sobre $m$ e $n$ para que $R$ seja uma aplicação?

**56.** Descreva todas as aplicações de $E = \{0, 1, 2\}$ em $F = \{3, 4\}$.

**57.** Descreva como conjunto de pares ordenados a função $f: E \to F$ dada pela lei:

$$f(x) = \begin{cases} 1, \text{ se } x \in \mathbb{Q} \\ -1, \text{ se } x \notin \mathbb{Q} \end{cases}$$

São dados: $E = \left\{0, 1, \frac{1}{2}, \sqrt{2}, \pi, \frac{7}{3}\right\}$ e $F = \mathbb{Z}$.

**58.** Seja $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $f(x, y) = \text{mdc}(x, y)$.
Determine $f(5, 1)$, $f(12, 8)$, $f(3, 7)$, $f(0, 5)$ e $f(0, 0)$.

**59.** A aplicação $f: \mathbb{R} \to \mathbb{R}$ é dada pela lei:

$$f(x) = \begin{cases} 2x + 5, \text{ se } x < -1 \\ x^2 + 2, \text{ se } -1 \leq x \leq 1 \\ 3x, \text{ se } x > 1 \end{cases}$$

Determine $f(0)$, $f\left(\frac{5}{3}\right)$, $f\left(-\frac{7}{2}\right)$, $f(\sqrt{3})$ e $f\left(-\frac{2\pi}{5}\right)$.

**60.** Decida em cada caso se $f$ e $g$ são funções iguais ou distintas.

1º) $f(x) = \dfrac{x^2 - 2x + 1}{x - 1}$, $g(x) = x - 1$ e $x \in \mathbb{R} - \{1\}$

2º) $f(x) = 1$, $g(x) = x^4$ e $x \in \{1, -1, i, -i\}$

3º) $f(x) = x^3$, $x \in \mathbb{R}$ e $g(y) = y^3$, $y \in [-1, 1]$

## 6. IMAGEM DIRETA — IMAGEM INVERSA

Seja uma aplicação $f: E \to F$.

**Definição 27:** Dado $A \subset E$, chama-se *imagem direta de* A, segundo $f$, e indica-se por $f(A)$, o seguinte subconjunto de $F$:

$$f(A) = \{f(x) \mid x \in A\}$$

isto é, $f(A)$ é o conjunto das imagens por $f$ dos elementos de $A$.

**Definição 28:** Dado $B \subset F$, chama-se imagem inversa de $B$, segundo $f$, e indica-se por $f^{-1}(B)$, o seguinte subconjunto de $E$:

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$

isto é, $f^{-1}(B)$ é o conjunto dos elementos de $E$ que têm imagem em $B$ através de $f$.

*Exemplos 20:*

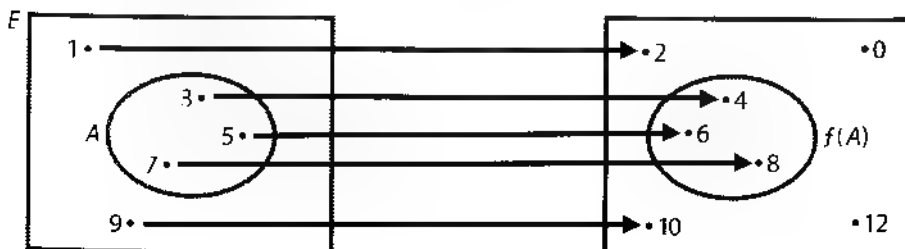
1º) Se $E = \{1, 3, 5, 7, 9\}$, $F = \{0, 2, 4, 6, 8, 10, 12\}$ e $f: E \to F$ é dada por $f(x) = x + 1$, temos:

$f(\{3, 5, 7\}) = \{f(3), f(5), f(7)\} = \{4, 6, 8\}$

$f(E) = \{f(1), f(3), f(5), f(7), f(9)\} = \{2, 4, 6, 8, 10\}$

$f(\varnothing) = \varnothing$

$f^{-1}(\{2, 4, 10\}) = \{x \in E \mid f(x) \in \{2, 4, 10\}\} = \{1, 3, 9\}$

$f^{-1}(\{0, 12\}) = \{x \in E \mid f(x) \in \{0, 12\}\} = \varnothing$

2º) Se $E = F = \mathbb{R}$ e $f: \mathbb{R} \to \mathbb{R}$ é dada pela lei $f(x) = x^2$, temos:

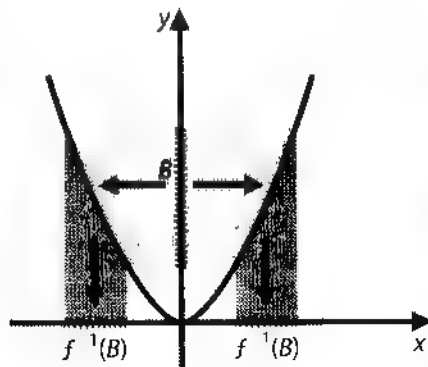
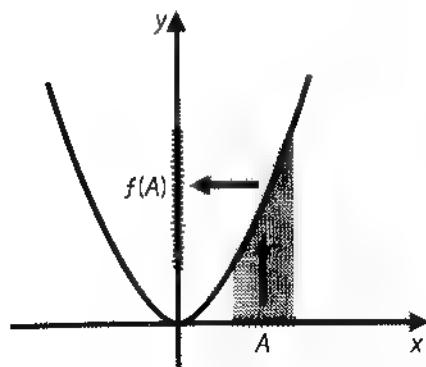
$f(\{1, 2, 3\}) = \{1, 4, 9\}$

$f([0, 2]) = \{f(x) \mid 0 \leqslant x \leqslant 2\} = \{x^2 \mid 0 \leqslant x \leqslant 2\} = [0, 4]$

$f(]-1, 3[) = \{x^2 \mid -1 < x < 3\} = [0, 9[$

$f^{-1}(\{0, 4, 16\}) = \{x \in \mathbb{R} \mid x^2 \in \{0, 4, 16\}\} = \{0, \pm 2, \pm 4\}$

$f^{-1}([1, 9]) = \{x \in \mathbb{R} \mid 1 \leqslant x^2 \leqslant 9\} = [-3, -1] \cup [1, 3]$

$f^{-1}(\mathbb{R}_-^*) = \{x \in \mathbb{R} \mid x^2 < 0\} = \varnothing$

3º) Seja $f: \mathbb{R} \to \mathbb{R}$ tal que:

$$f(x) = \begin{cases} 0, \text{ se } x \in \mathbb{Q} \\ 1, \text{ se } x \in \mathbb{R} - \mathbb{Q} \end{cases}$$

Temos:

$f(\mathbb{Q}) = \{f(x) \mid x \in \mathbb{Q}\} = \{0\}$

$f(\mathbb{R} - \mathbb{Q}) = \{f(x) \mid x \in \mathbb{R} - \mathbb{Q}\} = \{1\}$

$f([2, 3]) = \{f(x) \mid x \in [2, 3]\} = \{0, 1\}$

$f^{-1}(\{0\}) = \{x \in \mathbb{R} \mid f(x) = 0\} = \mathbb{Q}$

$f^{-1}([4, 5]) = \{x \in \mathbb{R} \mid f(x) \in [4, 5]\} = \varnothing$

## Exercícios

**61.** O diagrama abaixo representa a aplicação $f: E \to F$. Determine:

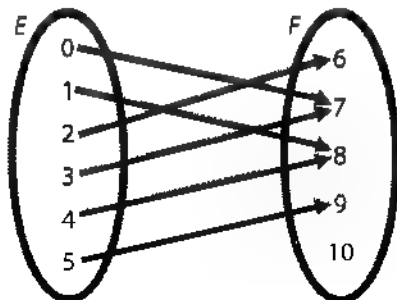
a) $f(\{0, 1\})$

b) $f(\{3, 4\})$

c) $f(\{1, 2, 5\})$

d) $f(E)$

e) $f^{-1}(\{7, 8\})$

f) $f^{-1}(\{10\})$

**62.** Considere a função $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = |x|$.

Determine:

a) $f(1)$
b) $f(-3)$
c) $f(1 - \sqrt{2})$
d) $f([-1, 1])$
e) $f(]-1, 2])$
f) $f(\mathbb{R})$
g) $f^{-1}([0, 3])$
h) $f^{-1}([-1, 3])$
i) $f^{-1}(\mathbb{R}^*_-)$

**63.** Seja $f: \mathbb{R} \to \mathbb{R}$, dada pela lei:

$$f(x) = \begin{cases} x^2, \text{ se } x \leq 0 \\ \sqrt[3]{x}, \text{ se } x > 0 \end{cases}$$

Determine:

a) $f([-1, 8])$
b) $f(\mathbb{R}_-)$
c) $f(\mathbb{R}_+)$
d) $f^{-1}([1, 16])$
e) $f^{-1}([-1, 16])$
f) $f^{-1}(\mathbb{R}^*_-)$

**64.** Seja $f: \mathbb{N}^* \times \mathbb{N} \to \mathbb{N}$ dada pela lei $f(x, y) = x^y$.

Determine:

a) $f(0, 2)$
b) $f(3, 0)$
c) $f(3, 4)$
d) $f^{-1}(\{16\})$
e) $f^{-1}(\{625\})$
f) $f^{-1}(\{1\})$
g) $f(1, \alpha)$, $\alpha \in \mathbb{N}$
h) $f^{-1}(\{p\})$, $p$ primo
i) $f^{-1}(\{0\})$

## 7. APLICAÇÕES INJETORAS — APLICAÇÕES SOBREJETORAS

Seja uma aplicação $f: E \to F$.

**Definição 29:** Dizemos que $f$ é uma *aplicação injetora* ou *injeção* se dois elementos diferentes quaisquer de $E$ têm imagens diferentes. Em outras palavras, se para quaisquer $x_1, x_2 \in F$, tais que $x_1 \neq x_2$, valer $f(x_1) \neq f(x_2)$.

Notemos que a contrapositiva da definição anterior é: se $x_1, x_2 \in E$ e $f(x_1) = f(x_2)$, então $x_1 = x_2$. Normalmente se usa essa contrapositiva, que é equivalente à definição, para verificar se $f$ é injetora ou não.

Negando-se a definição 29, obtém-se uma condição para que $f$ não seja injetora. Logo, $f$ *não é injetora* se existem $x_1, x_2 \in E$, tais que $x_1 \neq x_2$ e $f(x_1) = f(x_2)$.

**Definição 30:** Dizemos que $f$ é uma *aplicação sobrejetora* ou *sobrejeção* quando está verificada a seguinte condição:

$$\text{Im}(f) = F$$

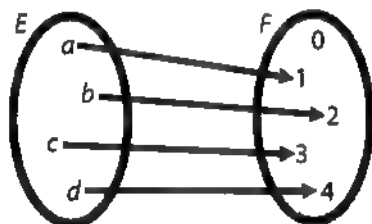
Observando-se que, para toda $f: E \to F$, tem-se $\text{Im}(f) \subset F$, então basta provar que $F \subset \text{Im}(f)$ para estabelecer que $f$ é sobrejetora. Ou seja, basta mostrar que para todo $y \in F$ existe $x \in E$ tal que $f(x) = y$.

Portanto, uma aplicação $f: E \to F$ *não é sobrejetora* se existe $y \in F$ tal que, qualquer que seja $x \in E$, $f(x) \neq y$.

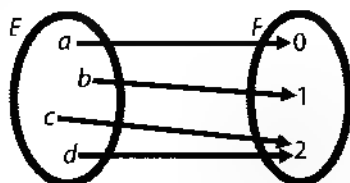
**Definição 31:** Dizemos que $f$ é uma *aplicação bijetora* ou *bijeção* quando $f$ é injetora e sobrejetora.

*Exemplos 21 e contra exemplos 6.*

1º) Se $E = \{a, b, c, d\}$ e $F = \{0, 1, 2, 3, 4\}$, a aplicação $f = \{(a, 1), (b, 2), (c, 3), (d, 4)\}$ de $E$ em $F$ é injetora.

Notemos que no esquema de flechas de uma aplicação injetora não há flechas que convergem para o mesmo elemento de $F$.

Podemos notar também que $f$ não é sobrejetora, pois $0 \in F$ e $0 \notin \text{Im}(f)$.

2º) Se $E = \{a, b, c, d\}$ e $F = \{0, 1, 2\}$, a aplicação $f = \{(a, 0), (b, 1), (c, 2), (d, 2)\}$ de $E$ em $F$ é sobrejetora.

Notemos que no esquema de flechas de uma aplicação sobrejetora todo elemento de $F$ serve de extremidade para alguma flecha.

Podemos notar também que $f$ não é injetora, pois $c \neq d$ e $f(c) = f(d) = 2$.

3º) A aplicação $f: \mathbb{R} \to \mathbb{R}$ dada pela lei $f(x) = 3x - 1$ é bijetora, pois:

(i) dados $x_1, x_2 \in \mathbb{R}$, temos:

$$f(x_1) = f(x_2) \Rightarrow 3x_1 - 1 = 3x_2 - 1 \Rightarrow x_1 = x_2$$

portanto, $f$ é injetora;

(ii) dado $y \in \mathbb{R}$, provemos que existe $x \in \mathbb{R}$ tal que $f(x) = y$:

$$3x - 1 = y \Rightarrow 3x = y + 1 \Rightarrow x = \frac{y + 1}{3} \in \mathbb{R}$$

portanto, $f$ é sobrejetora.

**Nota**

As aplicações não podem ser divididas em injetoras ou sobrejetoras. Há muitas e muitas aplicações que não são injetoras nem sobrejetoras. Por exemplo, a aplicação $f: \mathbb{R} \to \mathbb{R}$ dada pela lei $f(x) = x^2$ não é injetora, pois

$$2 \neq -2 \text{ e } f(2) = f(-2) = 4$$

e não é sobrejetora, pois

$$-1 \in \mathbb{R} \text{ e } \nexists x \in \mathbb{R} \mid x^2 = -1$$

## Exercícios

**65.** Quais das seguintes aplicações de $E = \{a, b, c, d, e\}$ em $F = \{0, 1, 2, 3, 4, 5\}$ são injetoras?

$f_1 = \{(a, 1), (b, 2), (c, 3), (d, 4), (e, 5)\}$
$f_2 = \{(a, 5), (b, 4), (c, 2), (d, 1), (e, 0)\}$
$f_3 = \{(a, 0), (b, 1), (c, 2), (d, 0), (e, 3)\}$
$f_4 = \{(a, 5), (b, 5), (c, 5), (d, 5), (e, 5)\}$

**66.** Quais das seguintes aplicações de $E = \{a, b, c, d, e\}$ em $F = \{1, 2, 3, 4\}$ são sobrejetoras?

$f_1 = \{(a, 1), (b, 2), (c, 3), (d, 1), (e, 3)\}$
$f_2 = \{(a, 2), (b, 1), (c, 3), (d, 3), (e, 4)\}$
$f_3 = \{(a, 3), (b, 3), (c, 1), (d, 2), (e, 1)\}$
$f_4 = \{(a, 4), (b, 4), (c, 2), (d, 3), (e, 1)\}$

**67.** Descreva uma a uma todas as aplicações injetoras de $E = \{a, b\}$ em $F = \{1, 2, 3\}$.

**68.** Descreva uma a uma todas as aplicações sobrejetoras de $E = \{a, b, c\}$ em $F = \{1, 2\}$.

**69.** Determine todas as aplicações bijetoras (ou permutações) de $E$ em $E$ sendo $E = \{a, b, c\}$ constituído por três elementos distintos.

**70.** Seja $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada pela lei $f(x, y) = \text{mdc}(x, y)$.

a) Determine: $f(2, 3)$, $f(0, 5)$ e $f(24, 36)$.
b) $f$ é injetora?
c) $f$ é sobrejetora?

**71.** Dê um argumento razoável para justificar que toda aplicação injetora de um conjunto finito $E$ em si mesmo é também sobrejetora.

**72.** Dê um argumento razoável para justificar que toda aplicação sobrejetora de um conjunto finito $E$ em si mesmo é também injetora.

**73.** Considere as seguintes funções de $\mathbb{R}$ em $\mathbb{R}$:

a) $y = 3$
b) $y = x + 2$
c) $y = x^2 - 5x + 6$
d) $y = 2^x$
e) $y = x^3$
f) $y = |x|$
g) $y = \text{sen } x$
h) $\begin{cases} y = \frac{1}{x}, \text{ se } x \neq 0 \\ y = 2, \text{ se } x = 0 \end{cases}$

Quais são injetoras?
Quais são sobrejetoras?

**74.** Prove que a aplicação $f: \mathbb{R}^2 \to \mathbb{R}^2$ tal que $f(x, y) = (\sqrt[3]{x}, y^5)$ é sobrejetora.

**75.** Mostre que a aplicação $f: \mathbb{Z} \to \mathbb{Z}$ dada pela lei $f(n) = 2n$, $n \in \mathbb{Z}$, é injetora mas não é sobrejetora.

**76.** Sendo $a, b, c, d$ inteiros, quais são as condições para que a aplicação $f: \mathbb{Z} \times \mathbb{Z} \to$ $\to \mathbb{Z} \times \mathbb{Z}$ tal que $f(x, y) = (ax + b, cy + d)$ seja injetora?

**77.** Prove que $f: \mathbb{R} \to \mathbb{R}$ definida por $f(x) = ax + b$, com $a$ e $b$ constantes reais e $a \neq 0$, é uma aplicação bijetora.

**78.** Mostre que $f: \mathbb{R} - \left\{\frac{d}{c}\right\} \to \mathbb{R} - \left\{\frac{a}{c}\right\}$ dada pela lei $y = \frac{ax - b}{cx - d}$, em que $a, b, c, d$ são constantes reais, $c \neq 0$ e $ad - bc \neq 0$, é uma aplicação bijetora.

**79.** Seja $f: \mathbb{R}^2 \to \mathbb{R}$ dada por $f(x, y) = xy$.

a) $f$ é injetora?

b) $f$ é sobrejetora?

c) Determine $f^{-1}(\{0\})$.

d) Determine $f([0, 1] \times [0, 2])$.

e) Determine $f(\{(x, y) \mid x = y\})$.

**80.** Considere a aplicação $f: \mathbb{Z}^2 \to \mathbb{Z}^2$ tal que $f(x, y) = (2x + 3, 4y + 5)$. Prove que $f$ é injetora. Verifique se $f$ é bijetora.

**81.** Dois conjuntos, $A$ e $B$, são *eqüipotentes* quando $A = B = \varnothing$ ou existe $f: A \to B$ bijetora. Mostre, em cada caso seguinte, que os conjuntos $A$ e $B$ são eqüipotentes.

1º) $A = \mathbb{N}$ e $B = \mathbb{N}^*$

2º) $A = \mathbb{Z}$ e $B = \mathbb{N}$

3º) $A = \mathbb{R}$ e $B = \mathbb{R}_+$

4º) $A = ]-1, 1[$ e $B = ]a, b[$, com $a$ e $b$ reais e $a < b$.

*Sugestão:* Descubra, em cada caso, $f: A \to B$ bijetora.

## 8. APLICAÇÃO INVERSA

Seja a aplicação $f: E \to F$. Por definição, $f$ é uma relação de $E$ em $F$ com certas particularidades:

(i) $D(f) = E$,

(ii) todo $x \in E$ tem imagem única $f(x) \in F$

Seja $f^{-1}$ a relação inversa de $f$. Pode acontecer que $f^{-1}$ não seja uma aplicação de $F$ em $E$. Voltando aos exemplos do item anterior, temos:

1º) $f = \{(a, 1), (b, 2), (c, 3), (d, 4)\}$

$f^{-1} = \{(1, a), (2, b), (3, c), (4, d)\}$

$f^{-1}$ não é aplicação de $F$ em $E$, pois $D(f^{-1}) = \{1, 2, 3, 4\} \neq F$.

2º) $f = \{(a, 0), (b, 1), (c, 2), (d, 2)\}$

$f^{-1} = \{(0, a), (1, b), (2, c), (2, d)\}$

$f^{-1}$ não é aplicação de $F$ em $E$, pois $(2, c) \in f^{-1}$ e $(2, d) \in f^{-1}$, sendo $c \neq d$.

O teorema seguinte estabelece em que condições $f^{-1}$ é uma aplicação.

**Proposição 5:** Seja $f: E \to F$ uma aplicação. Uma condição necessária e suficiente para que $f^{-1}$ seja uma aplicação de $F$ em $E$ é que $f$ seja bijetora.

*Demonstração:*

I. Provemos que, se $f^{-1}$ é aplicação, então $f$ é bijetora.

a) Sejam $x_1, x_2 \in E$, tais que $f(x_1) = y = f(x_2)$. Então $(x_1, y) \in f$ e $(x_2, y) \in f$ e, daí, $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$. Como $f^{-1}$ é aplicação, podemos escrever $x_1 = f^{-1}(y)$ e $x_2 = f^{-1}(y)$ e concluir, uma vez que $f^{-1}(y)$ é único, que $x_1 = x_2$. Está provado que $f$ é injetora.

b) Seja $y \in F$. Como $f^{-1}$ é aplicação de $F$ em $E$, existe $x \in E$ tal que $f^{-1}(y) = x$ e, portanto, $f(x) = y$. Está provado que $f$ é sobrejetora.

II. Provemos que, se $f$ é bijetora, então $f^{-1}$ é aplicação.

a) Como $f$ é sobrejetora, dado $y \in F$, existe $x \in E$ tal que $f(x) = y$ e, portanto, $(y, x) \in f^{-1}$. Está provado que $D(f^{-1}) = F$.

b) Seja $y \in F$ e suponhamos $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$. Então $(x_1, y) \in f$ e $(x_2, y) \in f$ ou considerando-se que $f$ é aplicação, $f(x_1) = y = f(x_2)$. Como, porém, $f$ é injetora, conclui-se dessas igualdades que $x_1 = x_2$. Isso mostra que, para cada $y \in F$, há um único elemento $x$ tal que $(y, x) \in f^{-1}$. De a) e b) segue que $f^{-1}$ é uma aplicação de $F$ em $E$. #

*Exemplo 22:*

Já vimos que a aplicação $f: \mathbb{R} \to \mathbb{R}$ tal que $f(x) = 3x - 1$ é bijetora. Determinemos a aplicação $f^{-1}$, inversa de $f$.

$$f^{-1} = \{(y, x) \in \mathbb{R}^2 \mid (x, y) \in f\} = \{(y, x) \in \mathbb{R}^2 \mid y = 3x - 1\} =$$
$$= \{(x, y) \in \mathbb{R}^2 \mid x = 3y - 1\} = \left\{(x, y) \in \mathbb{R}^2 \mid y = \frac{x + 1}{3}\right\}$$

portanto, $f^{-1}$ é a aplicação de $\mathbb{R}$ em $\mathbb{R}$ dada pela lei $f^{-1}(x) = \frac{x + 1}{3}$.

**Nota**

Pode ser provado que, se $f$ é bijetora, então $f^{-1}$ também é. Sendo $f^{-1}$ bijetora, a relação inversa de $f^{-1}$ também é aplicação. Mas $(f^{-1})^{-1} = f$; então $f$ e $f^{-1}$ são aplicações inversas uma da outra.

**Exercícios**

**82.** Determine a aplicação inversa de $f: \mathbb{R} \to \mathbb{R}$ definida por $f(x) = ax + b$, com $a$ e $b$ constantes reais e $a \neq 0$.

**83.** Descreva a aplicação inversa de $f: \mathbb{R} - \left\{\frac{d}{c}\right\} \to \mathbb{R} - \left\{\frac{a}{c}\right\}$ dada pela lei $f(x) = \frac{ax - b}{cx - d}$, em que $a, b, c, d$ são constantes reais, $c \neq 0$ e $ad - bc \neq 0$.

**84.** Descreva a aplicação inversa de $f: \mathbb{Z}^2 \to \mathbb{Z}^2$ dada por $f(x, y) = (x + 3, 2 - y)$.

## 9. COMPOSIÇÃO DE APLICAÇÕES

**Definição 32:** Sejam $f: E \to F$ e $g: F \to G$ duas aplicações. Chama-se *composta* de $f$ e $g$ a aplicação (indicada por $g \circ f$) de $E$ em $G$ definida da seguinte maneira:

$$(g \circ f)(x) = g(f(x))$$

para todo $x \in E$.

*Exemplos 23:*

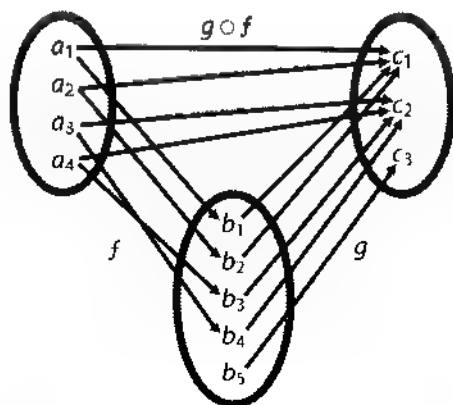
1º) Sejam $E = \{a_1, a_2, a_3, a_4\}$, $F = \{b_1, b_2, b_3, b_4, b_5\}$ e $G = \{c_1, c_2, c_3\}$. Consideremos as aplicações:

$f = \{(a_1, b_1), (a_2, b_2), (a_3, b_4), (a_4, b_3)\}$ de $E$ em $F$

$g = \{(b_1, c_1), (b_2, c_1), (b_3, c_2), (b_4, c_2), (b_5, c_3)\}$ de $F$ em $G$

A aplicação composta de $f$ e $g$, de acordo com a definição, é $g \circ f: E \to G$ tal que:

$$(g \circ f)(a_1) = g(f(a_1)) = g(b_1) = c_1$$
$$(g \circ f)(a_2) = g(f(a_2)) = g(b_2) = c_1$$
$$(g \circ f)(a_3) = g(f(a_3)) = g(b_4) = c_2$$
$$(g \circ f)(a_4) = g(f(a_4)) = g(b_3) = c_2$$

isto é, $g \circ f = \{(a_1, c_1), (a_2, c_1), (a_3, c_2), (a_4, c_2)\}$.

2º) Sendo $f: \mathbb{R} \to \mathbb{R}$ tal que $f(x) = 3x$ e $g: \mathbb{R} \to \mathbb{R}$ tal que $g(x) = x^2$, a aplicação composta de $f$ e $g$ é $g \circ f: \mathbb{R} \to \mathbb{R}$ tal que:

$$(g \circ f)(x) = g(f(x)) = (f(x))^2 = (3x)^2 = 9x^2$$

3º) Sejam $f: \mathbb{R} \to \mathbb{R}_+$ tal que $f(x) = 2^x$ e $g: \mathbb{R}_+ \to \mathbb{R}$ tal que $g(x) = \sqrt{x}$. A aplicação composta de $f$ e $g$ é $g \circ f: \mathbb{R} \to \mathbb{R}$ tal que:

$$(g \circ f)(x) = g(f(x)) = \sqrt{f(x)} = \sqrt{2^x}$$

**Notas**

I. A composta de $f$ e $g$ só está definida quando o contradomínio de $f$ coincide com o domínio de $g$ (conjunto $F$).

II. A composta de $f$ e $g$ tem o mesmo domínio de $f$ (conjunto $E$) e o mesmo contradomínio de $g$ (conjunto $G$).

III. Quando $E = G$, ou seja, $f: E \to F$ e $g: F \to E$, então é possível definir, além de $g \circ f$, a composta de $g$ e $f$ (indicada por $(f \circ g)$: é a aplicação de $F$ em $F$ que obedece à lei

$$(f \circ g)(x) = f(g(x))$$

para todo $x \in F$.

Retomando os exemplos anteriores, temos:

2º) A aplicação $f \circ g: \mathbb{R} \to \mathbb{R}$ é tal que:

$$(f \circ g)(x) = f(g(x)) = 3 \cdot g(x) = 3x^2$$

3º) A aplicação $f \circ g: \mathbb{R}_+ \to \mathbb{R}_+$ é tal que:

$$(f \circ g)(x) = f(g(x)) = 2^{g(x)} = 2^{\sqrt{x}}$$

IV. Se $f: E \to F$ e $g: F \to E$, então existem $g \circ f$ e $f \circ g$, mas pode ocorrer de $g \circ f \neq f \circ g$. Sugerimos ao estudante encontrar exemplos disso.

**Proposição 6:** $f: E \to F$ e $g: F \to G$ são injetoras, então $g \circ f$ é injetora.

*Demonstração:* Sejam $x_1, x_2 \in E$ tais que $(g \circ f)(x_1) = (g \circ f)(x_2)$. Então $g(f(x_1)) = g(f(x_2))$ e, como $g$ é injetora, $f(x_1) = f(x_2)$. Usando-se agora a hipótese de que $f$ é injetora, conclui-se que $x_1 = x_2$.

Logo, $g \circ f$ é injetora. #

**Proposição 7:** Se $f: E \to F$ e $g: F \to G$ são sobrejetoras, então $g \circ f$ é sobrejetora.

*Demonstração:* Seja $z \in G$. Como $g$ é sobrejetora, existe um $y \in F$ tal que $g(y) = z$. Sendo $f$ sobrejetora, existe um $x \in E$ tal que $f(x) = y$. Assim, temos:

$$z = g(y) = g(f(x)) = (g \circ f)(x)$$

Isso prova que $g \circ f$ é sobrejetora. #

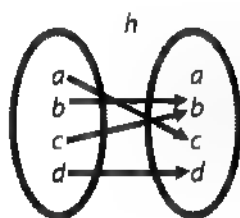
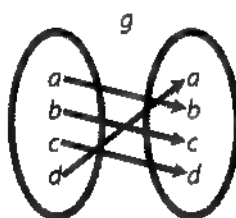
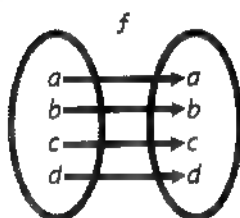
**Nota**

Quando compomos duas aplicações tais que uma é injetora e a outra é sobrejetora, de maneira geral nada podemos afirmar sobre a composta.

Veja o 1º exemplo, à página 103. Temos: $f$ injetora, $g$ sobrejetora e $g \circ f$ não injetora nem sobrejetora.

## Exercícios

**85.** Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ e $C = \{8, 9, 0\}$.
Seja $f: A \rightarrow B$ dada por $f(1) = 4$, $f(2) = 5$ e $f(3) = 6$.
Seja $g: B \rightarrow C$ dada por $g(4) = g(5) = 8$, $g(6) = 9$ e $g(7) = 0$.
Descreva pelos pares ordenados a aplicação $g \circ f$. A aplicação $g \circ f$ é injetora ou sobrejetora?

**86.** Considere as aplicações $f, g, h$, sobre $E = \{a, b, c, d\}$ dadas nos diagramas abaixo.
Determine as compostas $g \circ f$, $f \circ g$, $g \circ h$, $h \circ g$, $h \circ f$ e $h \circ h$.

**87.** Sejam $f, g, h$ funções de $\mathbb{R}$ em $\mathbb{R}$ definidas pelas leis $f(x) = x + 2$, $g(x) = x^2 - 1$ e $h(x) = 3x$.

a) Determine as compostas $f \circ g$, $f \circ h$, $g \circ f$, $g \circ g$, $g \circ h$ e $h \circ g$.

b) Verifique que $(f \circ g) \circ h = f \circ (g \circ h)$.

**88.** Considere as funções $f$ e $g$ de $\mathbb{R}$ em $\mathbb{R}$ definidas pelas regras $f(x) = x^3 + 1$ e $g(x) = x^2 + 1$. Determine as compostas $f \circ g$, $g \circ f$, $f \circ f$ e $g \circ g$.

**89.** Sendo $f(x) = ax^n$, com $n \in \mathbb{N}^*$, determine $a$ e $n$ de modo que $(f \circ f)(x) = 3x^4$.

**90.** Considere as funções $f: \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = 2x + 7$ e $f \circ g: \mathbb{R} \rightarrow \mathbb{R}$ dada por $(f \circ g)(x) = 4x^2 - 2x + 3$. Determine a função $g$.

**91.** Sejam $f$ e $g$ duas funções de $\mathbb{R}$ em $\mathbb{R}$ assim definidas:

$$f(x) = \begin{cases} x + 1, \text{ se } x \geqslant 0 \\ x + 1, \text{ se } x < 0 \end{cases} \quad \text{e} \quad g(x) = 3x - 2$$

Determine as compostas $f \circ g$ e $g \circ f$.

**92.** Sendo $f: \mathbb{R} \to \mathbb{R}$ uma função dada pela fórmula:

$$f(x) = \begin{cases} x + 1, \text{ se } x < 0 \\ 1 - 2x, \text{ se } x \geq 0 \end{cases}$$

Determine a composta $f \circ f$.

**93.** Determine as compostas $f \circ g$ e $g \circ f$, sabendo que $f$ e $g$ são funções de $\mathbb{R}$ em $\mathbb{R}$ tais que:

$$f(x) = \begin{cases} x^2, \text{ se } x < 0 \\ 2x, \text{ se } x \geqslant 0 \end{cases} \quad \text{e} \quad g(x) = \begin{cases} 1 - x, \text{ se } x < 1 \\ 1 + x, \text{ se } x \geqslant 1 \end{cases}$$

## 10. APLICAÇÃO IDÊNTICA

**Definição 33:** Dado $E \neq \emptyset$, chama-se *aplicação idêntica de* E a aplicação $i_E: E \to E$ dada pela lei $i_E(x) = x$, para todo $x \in E$.

Notemos que para cada $E$ existe uma aplicação idêntica $i_E$ e ainda que, se $E \neq F$, então $i_E \neq i_F$, por terem diferentes domínios.

**Proposição 8:** Se $f: E \to F$ é bijetora, então:

$$f \circ f^{-1} = i_F \ \text{ e } \ f^{-1} \circ f = i_E$$

*Demonstração:* Já vimos que se $f$ é bijetora, então $f^{-1}$ é uma aplicação de $F$ em $E$. Ademais, em virtude da definição de imagem de uma relação, são equivalentes as igualdades $f(x) = y$ e $f^{-1}(y) = x$. Daí,

$$f(f^{-1}(y)) = y \ \text{ e } \ f^{-1}(f(x)) = x$$

ou seja:

$$(f \circ f^{-1})(y) = y \ \text{ e } \ (f^{-1} \circ f)(x) = x$$

De onde, $f \circ f^{-1} = i_F$ e $f^{-1} \circ f = i_E$. #

**Proposição 9:** Se $f: E \to F$ e $g: F \to E$, então:

a) $f \circ i_E = f$, $i_F \circ f = f$, $g \circ i_F = g$ e $i_E \circ g = g$;

b) se $g \circ f = i_E$ e $f \circ g = i_F$, então $f$ e $g$ bijetoras e $g = f^{-1}$.

*Demonstração:*

a) Provemos, por exemplo, que $f \circ i_E = f$.

Como $f: E \to F$ e $i_E: E \to E$, então $D(f \circ i_E) = E = D(f)$.

Dado qualquer $x \in E$, temos:

$$(f \circ i_E)(x) = f(i_E(x)) = f(x)$$

Logo, $f \circ i_E = f$

b) Provemos, por exemplo, que $f$ é bijetora.

Sejam $x_1, x_2 \in E$ elementos tais que $f(x_1) = f(x_2)$. Então $g(f(x_1)) = g(f(x_2))$. Daí $(g \circ f)(x_1) = (g \circ f)(x_2)$ ou, levando-se em conta a hipótese, $i_E(x_1) = i_E(x_2)$.

De onde, $x_1 \quad x_2$, conclusão que garante ser $f$ uma aplicação injetora

Para mostrar que $f$ é sobrejetora, tomemos $y \in F$. Então $y \quad i_F(y) \quad (f \circ g)(y) =$
$= f(g(y)) = f(x)$, em que $x = g(y) \in E$. Portanto, $f$ é sobrejetora.

Provemos que $g = f^{-1}$.

Temos $D(f^{-1}) \quad F = D(g)$ e $f \circ g \quad i_F \quad f \circ f^{-1}$; logo, $f(g(x)) = f(f^{-1}(x))$, para todo $x \in F$.

Mas, como $f$ é injetora, resulta $g(x) = f^{-1}(x)$, para todo $x \in F$. #

## Exercícios

**94.** Sendo $f: \mathbb{R}^* \to \mathbb{R} - \{1\}$ tal que $f(x) = \dfrac{x+2}{x}$ e $g: \mathbb{R} - \{1\}$ em $\mathbb{R}^*$ tal que $g(x) = \dfrac{2}{x-1}$, determine $f \circ g$ e $g \circ f$. O que se conclui do resultado obtido?

**95.** Considere as aplicações de $\mathbb{R}$ em $\mathbb{R}$:

$$f(x) = x + 2 \text{ e } g(x) = x^2 - x$$

a) Determine as aplicações $f \circ g$, $f \circ f$ e $g \circ g$.

b) Descreva a aplicação $h$ tal que $f \circ h = h \circ f \quad i_{\mathbb{R}}$.

**96.** Sendo $f: \mathbb{N} \to \mathbb{N}$ dada pela lei $f(n) = n + 1$, mostre que há infinitas funções $g: \mathbb{N} \to \mathbb{N}$ tais que $g \circ f = i_{\mathbb{N}}$. A função $f$ é inversível ($f^{-1}$ é aplicação)?

**97.** Sendo $g: \mathbb{N} \to \mathbb{N}$ tal que $g(n) = \dfrac{n}{2}$ se $n$ é par e $g(n) \quad \dfrac{n+1}{2}$ se $n$ é ímpar, mostre que existem infinitas funções $h: \mathbb{N} \to \mathbb{N}$ tais que $g \circ f = i_{\mathbb{N}}$. A função $g$ é inversível?

**98.** Se $f: E \to E$ e $g: F \to E$ são tais que $g \circ f = i_E$, quais das seguintes afirmações são verdadeiras?

a) $g = f^{-1}$

b) $f$ é sobrejetora

c) $f$ é injetora

d) $g$ é injetora

e) $g$ é sobrejetora

**99.** Sejam as aplicações $f: E \to F$ e $g: F \to E$.

Prove que:

a) se $g \circ f$ é injetora, então $f$ é injetora;

b) se $f \circ g$ é sobrejetora, então $g$ é sobrejetora.

**100.** Sejam as aplicações $f: E \to F$, $g: E \to F$ e $h: F \to G$.
Prove que se $h$ é injetora e $h \circ g = h \circ f$, então $g = f$.

## 11. RESTRIÇÃO E PROLONGAMENTO DE UMA APLICAÇÃO

**Definição 34:** Seja $f: E \to F$ e seja $A \subset E$, com $A \neq \varnothing$. Chama-se *restrição de* f *ao subconjunto* A a aplicação $f \mid A: A \to F$ assim definida:

$$(f \mid A)(x) = f(x)$$

para todo $x \in A$.

**Definição 35:** Seja $f: E \to F$ e sejam $B \supset E$ e $C \supset F$. Chama-se *prolongamento de* f *ao conjunto* B toda aplicação $g: B \to C$ tal que $g(x) = f(x)$, para todo $x \in E$.

*Exemplos 24:*

1º) Consideremos $f: \mathbb{R}^* \to \mathbb{R}$ dada por $f(x) = \dfrac{1}{x}$.

Se $A = \{2, 4, 6, \ldots\}$, então $f \mid A = \left\{\left(2, \frac{1}{2}\right), \left(4, \frac{1}{4}\right), \left(6, \frac{1}{6}\right), \ldots\right\}$ é a restrição de $f$ ao conjunto $A$.

A função $g: \mathbb{R} \to \mathbb{R}$ dada por $g(0) = 1$ e $g(x) = f(x)$, $\forall x \in \mathbb{R}^*$, é um prolongamento de $f$ ao conjunto $\mathbb{R}$.

2º) Consideremos $f: \mathbb{C} \to \mathbb{R}_+$ dada por $f(x + yi) = \sqrt{x^2 + y^2}$.

Note que $f$ associa cada número complexo ao seu módulo.

Seja $g: \mathbb{R} \to \mathbb{R}_+$ dada por $g(x) = |x|$.

Então $g$ é a restrição de $f$ ao conjunto $\mathbb{R}$, pois, para todo $x \in \mathbb{R}$, temos:

$$f(x) = f(x + 0i) = \sqrt{x^2 + 0^2} = \sqrt{x^2} = |x| = g(x).$$

## 12. APLICAÇÕES MONÓTONAS

**Definição 36:** Sejam $E$ e $F$ dois conjuntos parcialmente ordenados e seja $f: E \to F$. Por comodidade, indicamos com o mesmo símbolo ($\leqslant$) as relações de ordem sobre $E$ e sobre $F$, mas pode não se tratar da mesma relação.

Dizemos que $f$ é uma *aplicação crescente* em $E$ se $f(x) \leqslant f(x')$ sempre que $x \leqslant x'$. Ou seja, $f$ é crescente se para quaisquer $x, x' \in E$, com $x \leqslant x'$, valer $f(x) \leqslant f(x')$.

Dizemos que $f$ é uma aplicação decrescente em $E$ se $f(x') \leqslant f(x)$ sempre que $x \leqslant x'$. Em outras palavras, $f$ é decrescente se para quaisquer $x, x' \in E$, com $x \leqslant x'$, valer $f(x') \leqslant f(x)$.

Uma aplicação crescente ou decrescente em $E$ será chamada *aplicação monótona* em $E$

**Definição 37:** Uma aplicação $f: E \to F$ é dita *aplicação estritamente monótona* em $E$ quando satisfaz a uma das seguintes proposições:

a) $f$ é *estritamente crescente*, isto é:

$$\text{se } x < x', \text{ então } f(x) < f(x')$$

quaisquer que sejam $x, x' \in E$.

b) $f$ é *estritamente decrescente*, isto é:

$$\text{se } x < x', \text{ então } f(x') < f(x)$$

quaisquer que sejam $x, x' \in E$.

*Exemplos 25:*

1º) A aplicação $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 2^x$ é estritamente crescente, pois:

$$x < x' \Rightarrow 2^x < 2^{x'}, \forall x, x' \in \mathbb{R}$$

2º) A aplicação $g: \mathbb{R} \to \mathbb{R}$ dada por $g(x) = 1 - x$ é estritamente decrescente, pois:

$$x < x' \Rightarrow -x' < -x \Rightarrow 1 - x' < 1 - x \Rightarrow g(x') < g(x)$$

para todos $x, x' \in \mathbb{R}$.

## Exercícios

**101.** Quais das funções abaixo são restrições de $f: \mathbb{R} \to \mathbb{R}$ tal que $f(x) = x^2$?

a) $g = \{(0, 0), (1, 1), (2, 4)\}$ de $\{0, 1, 2\}$ em $\{0, 1, 4\}$

b) $h(x) = x^2$ de $\mathbb{C}$ em $\mathbb{C}$

c) $i_{\{0, 1\}}$ (aplicação idêntica de $\{0, 1\}$)

**102.** Considere a função $f: \mathbb{R}_+ \to \mathbb{R}_+$ dada pela lei $f(x) = \sqrt{x}$. Descreva a restrição de $f$ ao conjunto $A = \{0, 1, 4, 9, 16, 25\}$.

**103.** Quais das funções abaixo são prolongamentos de $i_{\mathbb{Z}}$?

a) $f: \mathbb{R} \to \mathbb{Z}$ tal que $f(x) = [x]$ = maior inteiro menor ou igual a $x$

b) $i_{\mathbb{R}}$

c) $g: \mathbb{R} \to \mathbb{R}$ tal que $g(x) = [x]$

**104.** Considere a função $f = \{(0, 1), (1, 2), (2, 4), (3, 8), (4, 16)\}$ de $E = \{0, 1, 2, 3, 4\}$ em $F = \{1, 2, 4, 8, 16\}$. Dê uma função experimental que prolongue $f$ ao conjunto $\mathbb{R}$.

## Exercícios complementares

**C11.** Se $E$ e $F$ são conjuntos finitos que têm $m$ e $n$ elementos, respectivamente, quantas são as aplicações de $E$ em $F$?

**C12.** Seja $f: E \to F$ e sejam $A \subset E$ e $B \subset E$.

Prove que:

a) se $A \subset B$, então $f(A) \subset f(B)$

b) $f(A \cup B) = f(A) \cup f(B)$

c) $f(A \cap B) \subset f(A) \cap f(B)$

d) $A \subset f^{-1}(f(A))$ e $f(f^{-1}(B)) \subset B$

e) $f$ é bijetora se, e somente se, $f(A^C) = (f(A))^C$ para todo $A \subset E$

*Lembrete:* Se $L \subset Y$, o símbolo $L^C$ representa o complemento de $L$ em relação a $Y$.

**C13.** Prove que, se uma função $f: \mathbb{R} \to \mathbb{R}$ é inversível e seu gráfico é uma curva simétrica em relação à reta $y = x$, então $f = f^{-1}$.

Dê exemplos de funções $f$ tais que $f = f^{-1}$.

**C14.** Prove que $f: ]-1, 1[ \to \mathbb{R}$ definida pela lei $f(x) = \dfrac{x}{1 - |x|}$ é bijetora, ou seja, $]-1, 1[$ e $\mathbb{R}$ são conjuntos equipotentes.

**C15.** Sejam $f: E \to F$ e $g: F \to G$. Supondo $g$ bijetora, prove que $f$ é injetora se, e somente se, $g \circ f$ é injetora.

**C16.** Seja $f: E \to F$ e sejam $A \subset F$ e $B \subset F$. Prove que:

a) $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$

b) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

c) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

d) $f^{-1}(A^C) = (f^{-1}(A))^C$

e) $f$ é sobrejetora se, e somente se, $f^{-1}(A) \neq \varnothing$ para todo $A \subset F$

**C17.** Seja $E = \{a, b\}$, com $a \neq b$. Calcule:

a) o número de relações sobre $E$;

b) o número de relações de equivalência sobre $E$;

c) o número de relações de ordem sobre $E$;

d) o número de aplicações de $E$ em $E$;

e) o número de bijeções de $E$ em $E$.

# III-3 OPERAÇÕES — LEIS DE COMPOSIÇÃO INTERNAS

## 13. EXEMPLOS PRELIMINARES

1º) Consideremos a aplicação $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $f(x, y) = x + y$, ou seja, $f$ associa a cada par $(x, y)$ de números naturais a sua soma $x + y$. A aplicação $f$ é conhecida como *operação de adição sobre* $\mathbb{N}$.

2º) Pensemos na aplicação $g: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ tal que $g(x, y) = x \cdot y$. Ela associa a cada par $(x, y)$ de números reais o seu produto $x \cdot y$. A aplicação $g$ é conhecida como operação de multiplicação sobre $\mathbb{R}$.

3º) Consideremos a aplicação $h: \mathcal{P}(E) \times \mathcal{P}(E) \to \mathcal{P}(E)$, em que $\mathcal{P}(E)$ indica o conjunto das partes de $E$, tal que $h(X, Y) = X \cap Y$, ou seja, $h$ associa a cada par de conjuntos $(X, Y)$ a sua interseção $X \cap Y$. Essa aplicação é conhecida pelo nome *operação de interseção sobre* $\mathcal{P}(E)$.

## 14. CONCEITUAÇÃO

**Definição 37:** Sendo $E$ um conjunto não vazio, toda a aplicação $f: E \times E \to E$ recebe o nome *operação sobre* E (ou em $E$) ou *lei de composição interna sobre* E (ou em $E$).

Nas considerações de caráter geral que faremos a seguir neste parágrafo, uma operação $f$ sobre $E$ associa a cada par $(x, y)$ de $E \times E$ um elemento de $E$ que será simbolizado por $x * y$ (lê-se "$x$ estrela $y$"). Assim $x * y$ é uma forma de indicar $f(x, y)$. Diremos também que $E$ é um conjunto munido da operação $*$.

O elemento $x * y$ é chamado *composto* de x e y pela operação $*$. Os elementos $x$ e $y$ do composto $x * y$ são chamados *termos* do composto $x * y$. Os termos $x$ e $y$ do composto $x * y$ são chamados, respectivamente, *primeiro e segundo termos* ou então, *termo da esquerda e termo da direita.*

Outras notações poderão ser usadas para indicar uma operação sobre $E$.

a) *Notação aditiva*

Nesse caso, o símbolo da operação é $+$, a operação é chamada *adição*, o composto $x + y$ é chamado *soma*, e os termos $x$ e $y$ são as *parcelas*.

b) *Notação multiplicativa*

Nesse caso, o símbolo da operação é $\cdot$ ou a simples justaposição, a operação é chamada *multiplicação*, o composto $x \cdot y$ ou $xy$ é chamado *produto*, e os termos $x$ e $y$ são os *fatores*.

c) Outros símbolos utilizados para operações genéricas são: $\triangle, \top, \perp, \times, \otimes, \oplus$, etc.

Mais exemplos 25:

1º) A aplicação $f: \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$ tal que $f(x, y) = x^y$ é operação de *potenciação* sobre $\mathbb{N}^*$.

**Nota**

Quaisquer que sejam os naturais não nulos $x$ e $y$, o símbolo $x^y$ representa um natural não nulo; portanto, $f$ está bem definida.

Podemos notar que essa operação não pode ser estendida a $\mathbb{Z}^*$, porque, por exemplo, a imagem do par $(2, -1)$ seria $2^{-1} \notin \mathbb{Z}^*$.

2º) A aplicação $f: \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^*$ tal que $f(x, y) = \frac{x}{y}$ é a operação de *divisão* sobre $\mathbb{Q}^*$.

A operação de divisão pode ser estendida também a $\mathbb{R}^*$ e $\mathbb{C}^*$.

Deixamos como exercício ao leitor encontrar exemplos que mostrem que a divisao não é uma operação em $\mathbb{N}^*$ ou em $\mathbb{Z}^*$.

3º) A aplicação $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que $f(x, y) = x - y$ é a operação de *subtração* sobre $\mathbb{Z}$.

A operação de subtração pode ser estendida a $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

4º) A aplicação $f: E \times E \to E$, em que $E = M_{m \times n}(\mathbb{R})$ representa o conjunto das matrizes do tipo $m \times n$ com elementos reais, tal que $f(x, y) = x + y$ é a operação de *adição* sobre $M_{m \times n}(\mathbb{R})$.

5º) A aplicação $f: E \times E \to E$, em que $E = M_n(\mathbb{R})$ representa o conjunto das matrizes quadradas de ordem $n$ com elementos reais, tal que $f(x, y) = x \cdot y$ é a operação de *multiplicação* sobre $M_n(\mathbb{R})$.

6º) A aplicação $\varphi: E \times E \to E$, em que $E = \mathbb{R}^{\mathbb{R}}$ representa o conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$, tal que $\varphi(f, g) = f \circ g$ é a operação de *composição* sobre $\mathbb{R}^{\mathbb{R}}$.

## 15. PROPRIEDADES DAS OPERAÇÕES

Seja $*$ uma lei de composição interna em $E$. Vejamos algumas propriedades que $*$ pode apresentar.

### 15.1 Propriedade associativa

**Definição 38:** Dizemos que $*$ goza da *propriedade associativa* se

$$x * (y * z) = (x * y) * z,$$

quaisquer que sejam $x, y, z \in E$.

*Exemplos 26:*

1º) As adições em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ são operações que gozam da propriedade associativa. (Costuma-se dizer que "são operações associativas".)

$$(x + y) + z = x + (y + z), \quad \forall x, y, z$$

2º) As multiplicações em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ são operações associativas

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z$$

3º) A adição em $M_{m \times n}(\mathbb{R})$, conjunto das matrizes do tipo $m \times n$ com elementos reais, é operação associativa.

$$(X + Y) + Z = X + (Y + Z), \quad \forall X, Y, Z$$

4º) A multiplicação em $M_n(\mathbb{R})$ é operação associativa.

$$(XY)Z = X(YZ), \quad \forall X, Y, Z$$

5º) A composição de funções de $\mathbb{R}$ em $\mathbb{R}$ é operação associativa.

$$(f \circ g) \circ h = f \circ (g \circ h), \quad \forall f, g, h$$

*Contra-exemplos 7:*

1º) A potenciação em $\mathbb{N}^*$ não é operação associativa, pois:

$2 * (3 * 4) = 2^{(3^4)} = 2^{81}$

$(2 * 3) * 4 = (2^3)^4 = 2^{12}$

2º) A divisão em $\mathbb{R}^*$ não é operação associativa, pois:

$24 * (4 * 2) = 24 : (4 : 2) = 24 : 2 = 12$

$(24 * 4) * 2 = (24 : 4) : 2 = 6 : 2 = 3$

**Observação**

O fato de uma operação ser associativa possibilita indicar o composto de mais de dois elementos sem necessidade de usar os parênteses, uma vez que qualquer associação entre os elementos presentes conduz ao mesmo resultado. Por exemplo:

$2 + 4 + 6 + 7 = (2 + 4) + (6 + 7) = 2 + (4 + 6) + 7 = 2 + (4 + 6 + 7) = 19$

Se uma operação não é associativa, temos a obrigação de usar parênteses para indicar como deve ser calculado um composto de três ou mais elementos, pois, caso contrário, deixamos o composto sem significado. Por exemplo, em $\mathbb{R}^*$, $48 : 6 \,.\, 2 : 4$ não tem significado, pois:

$(48 : 6) : (2 : 4) = 8 : \frac{1}{2} = 16$

$((48 \,.\, 6) : 2) : 4 = (8 : 2) : 4 \quad 4 : 4 \quad 1$

$48 \cdot ((6 : 2) : 4) \quad 48 : (3 : 4) = 48 : \frac{3}{4} = 64$

## 15.2 Propriedade comutativa

**Definição 39:** Dizemos que $*$ goza da *propriedade comutativa* se

$$x * y = y * x,$$

quaisquer que sejam $x, y \in E$.

*Exemplos 27:*

1º) As adições em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ são operações que gozam da propriedade comutativa. (Costuma-se dizer que "são operações comutativas".)

$$x + y = y + x, \quad \forall x, y$$

2º) As multiplicações em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ são operações comutativas.

$$x \cdot y = y \cdot x, \quad \forall x, y$$

3º) A adição em $M_{m \times n}(\mathbb{R})$ é operação comutativa.

$$X + Y = Y + X, \quad \forall X, Y$$

*Contra-exemplos 8:*

1º) A potenciação em $\mathbb{N}^*$ não é comutativa, pois, por exemplo, $2^3 \quad 8$ e $3^2 \quad 9$.

2º) A divisão em $\mathbb{R}^*$ não é comutativa, pois, por exemplo, $3 : 6 = \frac{1}{2}$ e $6 : 3 \quad 2$.

3º) A subtração em $\mathbb{Z}$ não é comutativa, pois, por exemplo, $3 - 7 = -4$ e $7 - 3 = 4$

4º) A multiplicação em $M_2(\mathbb{R})$ não é comutativa, pois, por exemplo:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

e

$$\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix}$$

5º) A composição de funções em $\mathbb{R}^{\mathbb{R}}$ não é comutativa, pois, por exemplo, se $f(x) = 3x$ e $g(x) = x^2 + 1$, temos:

$$(f \circ g)(x) = f(g(x)) = 3(x^2 + 1) = 3x^2 + 3$$

e

$$(g \circ f)(x) = g(f(x)) = (3x)^2 + 1 = 9x^2 + 1$$

## Exercícios

**105.** Em cada caso a seguir, verifique se a operação $*$ sobre $E$ é associativa.

a) $E = \mathbb{R}$ e $x * y = \dfrac{x + y}{2}$

b) $E = \mathbb{R}$ e $x * y = x$

c) $E = \mathbb{R}_+$ e $x * y = \sqrt{x^2 + y^2}$

d) $E = \mathbb{R}$ e $x * y = \sqrt[3]{x^3 + y^3}$

e) $E = \mathbb{R}^*$ e $x * y = \dfrac{x}{y}$

f) $E = \mathbb{R}_+$ e $x * y = \dfrac{x + y}{1 + xy}$

g) $E = \mathbb{Z}$ e $x * y = xy + 2x$

h) $E = \mathbb{Q}$ e $x * y = x + xy$

i) $E = \mathbb{R}$ e $x * y = x + y - 2x^2y^2$

j) $E = \mathbb{R}$ e $x * y = x^2 + y^2 + 2xy$

**106.** Em cada caso a seguir está definida uma operação sobre $\mathbb{Z} \times \mathbb{Z}$. Verifique se ela é associativa:

a) $(a, b) * (c, d) = (ac, 0)$

b) $(a, b) \triangle (c, d) = (a + c, b + d)$

c) $(a, b) \perp (c, d) = (ac, ad + bc)$

d) $(a, b) \square (c, d) = (a + c, bd)$

e) $(a, b) \times (c, d) = (ac - bd, ad + bc)$

**107.** Consideremos a operação $*$ em $\mathbb{R}$ definida pela regra:

$$x * y = ax + by + cxy$$

em que $a, b, c$ são números reais dados.

Determine as condições sobre $a, b, c$ de modo que $*$ seja associativa.

**108.** Examine novamente as operações do exercício 105 e verifique quais são comutativas

**109.** Examine novamente as operações do exercício 106 e verifique quais são comutativas.

**110.** Retome a operação definida no exercício 107 e estabeleça as condições sobre $a, b, c$ de modo que $*$ seja comutativa.

## 15.3 Elemento neutro

**Definição 40:** Se existe $e \in E$ tal que $e * x = x$ para todo $x \in E$, dizemos que $e$ é um *elemento neutro à esquerda* para $*$.

Se existe $e \in E$ tal que $x * e = x$ para todo $x \in E$, dizemos que $e$ é um *elemento neutro à direita* para $*$.

Se $e$ é elemento neutro à direita e à esquerda para a operação $*$, dizemos simplesmente que $e$ é *elemento neutro* para essa operação.

*Exemplo 28:*

1º) O elemento neutro das adições em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ é o número 0, pois $0 + x = x = x + 0$ para qualquer número $x$.

2º) O elemento neutro das multiplicações em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ é o número 1, pois $1 \cdot x = x = x \cdot 1$ para qualquer número $x$.

3º) O elemento neutro da adição em $M_{m \times n}(\mathbb{R})$ é $0_{m \times n}$ (matriz nula do tipo $m \times n$), pois $0_{m \times n} + X = X = X + 0_{m \times n}$, qualquer que seja $X \in M_{m \times n}(\mathbb{R})$.

4º) O elemento neutro da multiplicação em $M_n(\mathbb{R})$ é $I_n$ (matriz identidade do tipo $n \times n$), pois $I_n X = X = X I_n$, qualquer que seja $X \in M_n(\mathbb{R})$.

5º) O elemento neutro da composição em $\mathbb{R}^{\mathbb{R}}$ é a função $i_{\mathbb{R}}$ (função idêntica em $\mathbb{R}$), pois $i_{\mathbb{R}} \circ f = f = f \circ i_{\mathbb{R}}$, qualquer que seja $f \in \mathbb{R}^{\mathbb{R}}$.

*Contra-exemplos 9:*

1º) A subtração em $\mathbb{Z}$ admite 0 como elemento neutro à direita pois $x - 0 = x$ para todo $x \in \mathbb{Z}$, mas não admite neutro à esquerda, pois não existe $e$ (fixo) tal que $e - x = x$ para todo $x \in \mathbb{Z}$.

2º) A divisao em $\mathbb{R}^*$ admite 1 como elemento neutro à direita, pois $x : 1 = x$ para todo $x \in \mathbb{R}^*$, mas não admite neutro à esquerda, pois não existe $e$ (fixo) tal que $e : x = x$ para todo $x \in \mathbb{R}^*$.

3º) Todos os elementos de $\mathbb{R}$ são elementos neutros à esquerda da operaçao definida por $x * y = y$ sobre esse conjunto. De fato, se $e \in \mathbb{R}$, então $e * y = y$, qualquer que seja $y \in \mathbb{R}$ Mas nenhum numero real é elemento neutro à direita para essa operação De fato, se $e \in \mathbb{R}$ e $a$ é um número real diferente de $e$, entao $a * e \neq e$.

**Proposição 10:** Se a operação $*$ sobre $E$ tem um elemento neutro $e$, então ele é único.

*Demonstração:* Suponhamos que $e$ e $e'$ sejam elementos neutros da operação $*$.

Como $e$ e elemento neutro e $e' \in E$, então $e * e' = e'$. Por raciocínio análogo, chega-se à conclusão de que $e * e' = e$.

De onde, $e' = e$. #

## Exercícios

**111.** Examine novamente as operações do exercício 105 e determine quais têm elemento neutro.

**112.** Examine novamente as operações do exercício 106 e determine quais têm elemento neutro.

**113.** Determine todos os elementos neutros à esquerda para a operação de multiplicação em $E = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \; a, b \in \mathbb{R}\right\}$.

**114.** Estabeleça as condições sobre $m, n \in \mathbb{Z}$ de modo que a operação $*$ sobre $\mathbb{Z}$ dada pela lei $x * y = mx + ny$:

a) seja associativa;

b) seja comutativa;

c) admita elemento neutro.

**115.** Examine novamente a operação definida no exercício 107 e estabeleça as condições sobre $a, b, c$ de modo que a operação tenha elemento neutro.

## 15.4 Elementos simetrizáveis

**Definição 41:** Seja $*$ uma operação sobre $E$ que tem elemento neutro $e$. Dizemos que $x \in E$ é um *elemento simetrizável* para essa operação se existir $x' \in E$ tal que

$$x' * x = e = x * x'$$

O elemento $x'$ é chamado *simétrico de* x para a operação $*$.

Quando a operação é uma adição, o simétrico de $x$ também é chamado *oposto de* x e indicado por $-x$.

Quando a operação é uma multiplicação, o simétrico de $x$ também é chamado *inverso de* x e indicado por $x^{-1}$.

*Exemplos 29 e contra-exemplos10:*

1º) 3 é um elemento simetrizável para a adição em $\mathbb{Z}$, e seu simétrico (ou oposto) é $-3$, pois,

$$(-3) + 3 = 0 = 3 + (-3)$$

2º) 3 é um elemento simetrizável para a multiplicação em $\mathbb{Q}$, e seu simétrico (ou inverso) é $\frac{1}{3}$, pois:

$$\frac{1}{3} \cdot 3 = 1 = 3 \cdot \frac{1}{3}$$

0 *não* é simetrizável para a mesma operação, pois não há elemento $x' \in \mathbb{Q}$ ta que:

$$x' \cdot 0 = 1 = 0 \cdot x'$$

3º) Existem apenas dois elementos simetrizáveis para a multiplicação em $\mathbb{Z}$: o 1 e o $-1$, que são iguais aos seus respectivos inversos.

Já o 3 *não* é simetrizável para a multiplicação em $\mathbb{Z}$, uma vez que não existe $x' \in \mathbb{Z}$ tal que $x' \cdot 3 = 1 = 3 \cdot x'$.

4º) $\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$ é simetrizável para a adição em $M_2(\mathbb{R})$, e seu simétrico é $\begin{pmatrix} 1 & -2 \\ 3 & -6 \end{pmatrix}$, pois.

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} + \begin{pmatrix} 1 & -2 \\ 3 & 6 \end{pmatrix}$$

5º) $\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$ *não* é simetrizável para a multiplicação em $M_2(\mathbb{R})$, pois, supondo que sua inversa pudesse ser $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, teríamos:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} a + 3b & 2a + 6b \\ c + 3d & 2c + 3d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{cases} a + 3b = 1 \\ 2a + 6b = 0 \\ c + 3d = 0 \\ 2c + 6d = 1 \end{cases}$$

e esse sistema não tem solução.

6º) $\begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$ é simetrizável para a multiplicação em $M_2(\mathbb{R})$, e seu inverso é $\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$, pois:

$$\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$$

7º) A função de $\mathbb{R}$ em $\mathbb{R}$ dada pela lei $f(x) = 3x - 1$ é bijetora e, conseqüentemente, é inversível. Sua inversa é $f^{-1}(x) = \frac{x+1}{3}$. Temos:

$$f^{-1} \circ f = i_{\mathbb{R}} = f \circ f^{-1}$$ (lembre-se de que $i_{\mathbb{R}}$ é o neutro)

portanto, $f$ é um elemento de $\mathbb{R}^{\mathbb{R}}$, simetrizável para a composiçao de funçoes

Já qualquer função de $\mathbb{R}$ em $\mathbb{R}$ que não seja bijetora não é inversível e, portanto, não é elemento de $\mathbb{R}^{\mathbb{R}}$ simetrizável para a mesma operação.

**Proposição 11:** Seja $*$ uma operação sobre $E$ que é associativa e tem elemento neutro $e$.

a) Se um elemento $x \in E$ é simetrizável, então o simétrico de $x$ é único.

b) Se $x \in E$ é simetrizável, então seu simétrico $x'$ também é e $(x')' = x$.

c) Se $x, y \in E$ são simetrizáveis, então $x * y$ é simetrizável e $(x * y)' = y' * x'$.

*Demonstração:*

a) Suponhamos que $x'$ e $x''$ sejam simétricos de $x$. Temos:

$$x' = e * x' = (x'' * x) * x' = x'' * (x * x') = x'' * e = x''$$

b) Sendo $x'$ o simétrico de $x$, temos:

$$x' * x = e = x * x'$$

e, pela definição 41, $x$ é o simétrico de $x'$, ou seja, $x = (x')'$.

c) Para provarmos que $y' * x'$ é o simétrico de $x * y$, devemos mostrar que:

(1) $(y' * x') * (x * y) = e$

(2) $(x * y) * (y' * x') = e$

De fato, temos:

(1) $(y' * x') * (x * y) - [(y' * x') * x] * y - [y' * (x' * x)] * y \quad (y' * e) * y - y' * y \quad e$

(2) Analogamente. #

Por indução, pode-se generalizar a propriedade c): se $a_1, a_2, \quad , a_n$ são elementos de $E$, então $(a_1 * a_2 * \ldots * a_n)' \quad a'_n * a'_n \quad {}_1 * \ldots a'_2 * a'_1$.

**Notação: conjunto dos simetrizáveis**

Se $*$ é uma operação sobre $E$ com elemento neutro $e$, indica se por $U_*(E)$ o conjunto dos elementos simetrizáveis de $E$ para a operação $*$.

$$U_*(E) = \{x \in E \mid \exists x' \in E : x' * x = e = x * x'\}$$

*Exemplos 30:*

$U_+(\mathbb{N}) = \{0\}$

$U_+(\mathbb{Z}) = \mathbb{Z}$

$U_\cdot(\mathbb{Z}) = \{1, -1\}$

$U_\cdot(\mathbb{R}) = \mathbb{R}^*$

$U_+(M_n(\mathbb{R})) = M_n(\mathbb{R})$

$U_\cdot(M_n(\mathbb{R})) = \{X \in M_n(\mathbb{R}) \mid \det X \neq 0\}$

$U_0(\mathbb{R}^{\mathbb{R}}) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ é bijetora}\}$

Podemos notar que $U_*(E) \neq \varnothing$, pois necessariamente $e \in U_*(E)$, uma vez que $e * e \quad e$.

## Exercícios

**116.** Examine novamente as operações do exercício 105 que têm elemento neutro para determinar os elementos simetrizáveis.

**117.** Examine novamente as operações do exercício 106 que têm elemento neutro para determinar os elementos simetrizáveis.

**118.** Sendo $*$ a operação sobre $\mathbb{Z}^3$ dada por $(a, b, c) * (d, e, f) = (ad, be, cf)$, determine seu elemento neutro e o conjunto dos elementos simetrizáveis de $\mathbb{Z}^3$ para $*$.

**119.** Sejam $E$ e $F$ dois conjuntos em que estão definidas as operações $*$ e $\triangle$, respectivamente, as quais são associativas e têm neutros. Sobre o conjunto $E \times F$, consideremos uma operação $\circ$ assim definida:

$$(a, b) \circ (c, d) = (a * c, b \triangle d)$$

a) Mostre que $\circ$ é associativa e possui elemento neutro

b) Determine os elementos inversíveis de $E \times F$ para essa operação.

### 15.5 Elementos regulares

**Definição 42:** Seja $*$ uma operação sobre $E$. Dizemos que um elemento $a \in E$ e *regular* (*ou simplificável ou que cumpre a lei do cancelamento*) à esquerda em relação à operação $*$ se, para quaisquer $x, y \in E$ tais que $a * x = a * y$, vale $x = y$.

Dizemos que um elemento $a \in E$ é *regular* (*ou simplificável*) *à direita* relativamente à operação $*$ se, para quaisquer $x, y \in E$ tais que $x * a = y * a$, vale $x = y$.

Se $a \in E$ é um elemento regular à esquerda e à direita para a operação $*$, dizemos simplesmente que $a$ é *regular* para essa operação.

*Exemplos 31 e contra-exemplos 11:*

1º) 3 é regular para a adição em $\mathbb{N}$, pois:

$$3 + x = 3 + y \Rightarrow x = y$$

quaisquer que sejam $x, y \in \mathbb{N}$.

2º) 3 é regular para a multiplicação em $\mathbb{Z}$, pois:

$$3 \cdot x = 3 \cdot y \Rightarrow x = y$$

quaisquer que sejam $x, y \in \mathbb{Z}$.

3º) 0 *não* é regular para a multiplicação em $\mathbb{Z}$, pois:

$$0 \cdot 2 = 0 \cdot 3 \text{ e } 2 \neq 3$$

4º) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ é regular para a adição em $M_2(\mathbb{R})$, pois:

se $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, então $\begin{pmatrix} 1+a & 2+b \\ 3+c & 4+d \end{pmatrix} = \begin{pmatrix} 1+a' & 2+b' \\ 3+c' & 4+d' \end{pmatrix}$

e, daí, ($a = a'$, $b = b'$, $c = c'$ e $d = d'$). De onde $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$.

5º) $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ *não* é regular para a multiplicação em $M_2(\mathbb{R})$, pois

$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 4 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} \text{ e } \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \neq \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$$

**Proposição 12:** Se a operação $*$ sobre $E$ é associativa, tem elemento neutro $e$ e um elemento $a \in E$ é simetrizável, então $a$ é regular.

*Demonstração:* Sejam $x$ e $y$ elementos quaisquer de $E$ tais que $a * x = a * y$ e $x * a = y * a$.

Da primeira dessas hipóteses, segue que $a' * (a * x) = a' * (a * y)$. Daí, considerando-se a associatividade, $(a' * a) * x = (a' * a) * y$, ou seja, $e * x = e * y$. De onde, $x = y$.

Analogamente se prova que, se $x * a = y * a$, então $x = y$. Portanto, $a$ é regular. #

**Notação: conjunto dos regulares**

Sendo $*$ uma operação sobre $E$, indica-se com $R_*(E)$ o conjunto dos elementos regulares de $E$ para a operação $*$.

*Exemplos 32:*

$R_+(\mathbb{N}) = \mathbb{N}$

$R_\cdot(\mathbb{Z}) = \mathbb{Z}^*$

$R_+(M_2(\mathbb{R})) = M_2(\mathbb{R})$

Podemos notar que, se $*$ tem elemento neutro $e$, então $e \in R_*(E)$ e, portanto, $R_*(E) \neq \varnothing$.

Podemos notar também que, se $*$ é associativa e tem elemento neutro $e$, então $U_*(E) \subset R_*(E)$, conforme mostrou a proposição 12.

## Exercícios

**120.** Determine o conjunto dos elementos regulares para cada operação definida no exercício 105.

**121.** Determine os elementos regulares de $\mathbb{Z} \times \mathbb{Z}$ para cada operação definida no exercício 106.

**122.** Mostre que nenhum elemento de $\mathbb{R}$ é regular para a operação $*$ assim definida:

$$x * y = x^2 + y^2 - xy$$

**123.** Determine os elementos regulares de $\mathbb{R}$ relativamente à operação $*$ assim definida: $x*y \quad 5x + 3y \quad 7xy$.

**124.** Mostre que se $*$ é uma operação associativa sobre $E$, então $R(E) = \varnothing$ ou $\mathbb{R}_*(E)$ é subconjunto de $E$ fechado para a operação $*$.

### 15.6 Propriedade distributiva

**Definição 43:** Sejam $*$ e $\triangle$ duas operações sobre $E$. Dizemos que $\triangle$ é *distributiva à esquerda* relativamente a $*$ se:

$$x \triangle (y * z) = (x \triangle y) * (x \triangle z)$$

quaisquer que sejam $x, y, z \in E$.

Dizemos que $\triangle$ é *distributiva à direita* relativamente a $*$ se:

$$(y * z) \triangle x = (y \triangle x) * (z \triangle x)$$

quaisquer que sejam $x, y, z \in E$.

Quando $\triangle$ é distributiva à esquerda e à direita de $*$, dizemos simplesmente que $\triangle$ é *distributiva* relativamente a $*$.

*Exemplos 33:*

1º) A multiplicação em $\mathbb{Z}$ é distributiva em relação à adição em $\mathbb{Z}$, pois:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

quaisquer que sejam $x, y, z \in \mathbb{Z}$.

2º) A multiplicação em $M_n(\mathbb{R})$ é distributiva em relação à adição em $M_n(\mathbb{R})$, pois:

$$X \cdot (Y + Z) = (X \cdot Y) + (X \cdot Z)$$

$$(Y + Z) \cdot X = (Y \cdot X) + (Z \cdot X)$$

quaisquer que sejam $X, Y, Z \in M_n(\mathbb{R})$.

3º) Em $\mathbb{N}^*$, a potenciação é distributiva à direita em relação à multiplicação, pois:

$$(x \cdot y)^z = x^z \cdot y^z$$

quaisquer que sejam $x, y, z \in \mathbb{N}^*$.

Entretanto, a potenciação em $\mathbb{N}^*$ *não* é distributiva à esquerda em relação à multiplicação, pois, por exemplo:

$$2^{3 \cdot 4} \neq 2^3 \cdot 2^4$$

## 16. PARTE FECHADA PARA UMA OPERAÇÃO

**Definição 44:** Sejam $*$ uma operação sobre $E$ e $A$ um subconjunto não vazio de $E$. Dizemos que $A$ é uma parte fechada de $E$ para a operação $*$ se, e somente se, para quaisquer $x, y \in A$ verificar-se $x*y \in A$.

*Exemplos 34:*

1º) O conjunto $\mathbb{N}$ é uma parte fechada para a adição e a multiplicação em $\mathbb{Z}$, pois:

$$\mathbb{N} \neq \varnothing, \mathbb{N} \subset \mathbb{Z}$$

e

$$x \in \mathbb{N} \text{ e } y \in \mathbb{N} \Rightarrow x + y \in \mathbb{N}$$

$$x \in \mathbb{N} \text{ e } y \in \mathbb{N} \Rightarrow x \cdot y \in \mathbb{N}$$

quaisquer que sejam $x, y \in \mathbb{N}$.

2º) O conjunto $\mathbb{Q}$ é uma parte fechada para a adição e a multiplicação em $\mathbb{R}$, pois:

$$\mathbb{Q} \neq \varnothing, \mathbb{Q} \subset \mathbb{R}$$

e

$$x \in \mathbb{Q} \text{ e } y \in \mathbb{Q} \Rightarrow x + y \in \mathbb{Q}$$

$$x \in \mathbb{Q} \text{ e } y \in \mathbb{Q} \Rightarrow x \cdot y \in \mathbb{Q}$$

quaisquer que sejam $x, y \in \mathbb{Q}$.

3º) O conjunto $\mathbb{R}_+$ é uma parte fechada de $\mathbb{R}$ para a operação de multiplicação em $\mathbb{R}$, pois:

$$\mathbb{R}_+ \neq \varnothing, \mathbb{R}_+ \subset \mathbb{R} \text{ e } (x \in \mathbb{R}_+ \text{ e } y \in \mathbb{R}_+) \Rightarrow x \cdot y \in \mathbb{R}_+$$

quaisquer que sejam $x, y \in \mathbb{R}_+$.

4º) O conjunto $D_2(\mathbb{R})$ das matrizes diagonais do tipo $2 \times 2$ é uma parte fechada de $M_2(\mathbb{R})$ para a adição e a multiplicação em $M_2(\mathbb{R})$, pois:

$$\begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b' \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & a'+b' \end{pmatrix} \in D_2(\mathbb{R})$$

$$\begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & b' \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & a'b' \end{pmatrix} \in D_2(\mathbb{R})$$

quaisquer que sejam $a, a', b, b' \in \mathbb{R}$.

5º) O conjunto $A$ das funções bijetoras de $\mathbb{R}$ em $\mathbb{R}$ é um subconjunto fechado para a composição de funções em $\mathbb{R}^{\mathbb{R}}$, pois:

$$f \in A \text{ e } g \in A \Rightarrow f \circ g \in A$$

quaisquer que sejam $f, g \in A$.

*Contra-exemplos 12:*

1º) O conjunto $\mathbb{Z}_-$ é uma parte fechada para a adição em $\mathbb{R}$, mas *não* é parte fechada para a multiplicação, pois, por exemplo.

$$-2 \in \mathbb{Z}_-, -3 \in \mathbb{Z}_- \text{ e } (-2)(-3) \notin \mathbb{Z}_-$$

2º) O conjunto $\mathbb{R} - \mathbb{Q}$ (dos números irracionais) *não* é parte fechada para a adição em $\mathbb{R}$ e para a multiplicação em $\mathbb{R}$, pois, por exemplo:

$$\sqrt{2} \in \mathbb{R} - \mathbb{Q}, \ -\sqrt{2} \in \mathbb{R} - \mathbb{Q} \text{ e } (\sqrt{2}) + (-\sqrt{2}) \notin \mathbb{R} - \mathbb{Q}$$

$$\text{e } (\sqrt{2})(\sqrt{2}) \notin \mathbb{R} - \mathbb{Q}$$

3º) O conjunto $GL_2(\mathbb{R})$ das matrizes inversíveis *não* é fechado para a adição em $M_2(\mathbb{R})$, pois, por exemplo.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}), \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in GL_2(\mathbb{R}) \text{ e } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin GL_2(\mathbb{R})$$

## Exercícios

**125.** Em $\mathbb{Z} \times \mathbb{Z}$ estão definidas duas operações $*$ e $\triangle$ da seguinte forma:

$$(a, b) * (c, d) = (a + c, b + d)$$
$$(a, b) \triangle (c, d) = (ac, ad + bc)$$

Verifique se $\triangle$ é distributiva em relação a $*$.

**126.** Determine $m \in \mathbb{R}$ de modo que a operação $\triangle$ seja distributiva em relação à operação $*$, sendo $\triangle$ e $*$ definidas em $\mathbb{R}$ por:

$$x \triangle y = my$$
$$x * y = x + y + xy$$

**127.** Decida quais dos conjuntos abaixo são partes fechadas de $\mathbb{Z}$ para a operação de adição usual?

a) $\mathbb{Z}$
b) $P = \{x \in \mathbb{Z} \mid x \text{ é par}\}$
c) $I = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$
d) $J = \{x \in \mathbb{Z} \mid x \text{ é primo}\}$
e) $K = \{x \in \mathbb{Z} \mid \text{mdc}(x, 10) = 1\}$
f) $L = \{x \in \mathbb{Z} \mid x = 3q + 1, q \in \mathbb{Z}\}$

**128.** Repita o exercício anterior substituindo a adição pela multiplicação usual.

**129.** Mostre que $A = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$ é parte fechada de $M_2(\mathbb{R})$ para a operação de adição.

**130.** Mostre que $A = \left\{\begin{pmatrix} \cos a & \text{sen } a \\ -\text{sen } a & \cos a \end{pmatrix} \mid a \in \mathbb{R}\right\}$ é subconjunto de $M_2(\mathbb{R})$ fechado para a multiplicação.

**131.** Mostre que $A = \{z \in \mathbb{C} \mid z = \cos \theta + i \cdot \text{sen } \theta\}$ é subconjunto de $\mathbb{C}$ fechado para a multiplicação.

## 17. TÁBUA DE UMA OPERAÇÃO

**Como se constrói**

Seja $E = \{a_1, a_2, ..., a_n\}$, com $n > 1$, um conjunto com $n$ elementos. Toda operaçao sobre $E$ é uma aplicação $f: \mathbb{E} \times \mathbb{E} \to \mathbb{E}$ que associa a cada par $(a_i, a_j)$ o elemento $a_i * a_j = a_{ij}$.

Podemos representar o elemento $a_{ij}$, correspondente ao par $(a_i, a_j)$, numa tabela de dupla entrada construída como segue.

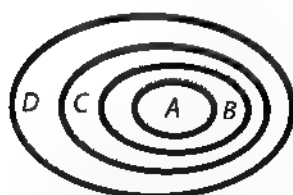
1º) Marcamos na linha fundamental e na coluna fundamental os elementos do conjunto $E$. Chamamos de $i$-ésima linha aquela que começa com $a_i$ e de $j$-ésima coluna a que é encabeçada por $a_j$.

2º) Dado um elemento $a_i$ na coluna fundamental e um elemento $a_j$ na linha fundamental, na interseção da $i$-ésima linha com a $j$-ésima coluna, marcamos o composto $a_{ij}$.

*Exemplos 35.*

1º) Tábua da multiplicação em $E \quad \{ \quad 1, 0, 1\}$.

| $\cdot$ | 1 | 0 | 1 |
|---|---|---|---|
| $-1$ | 1 | 0 | $-1$ |
| 0 | 0 | 0 | 0 |
| 1 | $-1$ | 0 | 1 |

2º) Tábuas das operações de reunião e de interseção sobre $E = \{A, B, C, D\}$, em que $A, B, C, D$ são conjuntos tais que $A \subset B \subset C \subset D$.

| $\cup$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $B$ | $C$ | $D$ |
| $B$ | $B$ | $B$ | $C$ | $D$ |
| $C$ | $C$ | $C$ | $C$ | $D$ |
| $D$ | $D$ | $D$ | $D$ | $D$ |

| $\cap$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $A$ | $A$ | $A$ |
| $B$ | $A$ | $B$ | $B$ | $B$ |
| $C$ | $A$ | $B$ | $C$ | $C$ |
| $D$ | $A$ | $B$ | $C$ | $D$ |

3º) Tábua operação $*$ sobre $E = \{1, 3, 5, 15\}$ tal que $x * y \quad \text{mdc}(x, y)$

| $*$ | 1 | 3 | 5 | 15 |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 3 | 1 | 3 |
| 5 | 1 | 1 | 5 | 5 |
| 15 | 1 | 3 | 5 | 15 |

4º) Tábua da operação de composição sobre $E = \{f_1, f_2, f_3\}$, em que $f_1, f_2, f_3$ são funções assim descritas:

$f_1 = \{(a, a), (b, b), (c, c)\}$
$f_2 = \{(a, b), (b, c), (c, a)\}$
$f_3 = \{(a, c), (b, a), (c, b)\}$

| $\circ$ | $f_1$ | $f_2$ | $f_3$ |
|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ |
| $f_2$ | $f_2$ | $f_3$ | $f_1$ |
| $f_3$ | $f_3$ | $f_1$ | $f_2$ |

## Exercícios

**132.** Em cada caso a seguir está definida uma operação $*$ sobre $E$ Faça a tábua da operação.

a) $E = \{1, 2, 3, 6\}$ e $x * y = \text{mdc}(x, y)$

b) $E = \{1, 3, 9, 27\}$ e $x * y = \text{mmc}(x, y)$

c) $E = \left\{1, \sqrt{2}, \frac{3}{2}\right\}$ e $x * y = \min(x, y)$

d) $E = \left\{3\sqrt{2}, \pi, \frac{7}{2}\right\}$ e $x * y = \max(x, y)$

e) $E = \{1, i, -1, -i\}$ e $x * y = x \cdot y$

**133.** Em cada caso a seguir está definida uma operação $*$ sobre $E = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$. Construa a tábua da operação.

a) $x * y = x \cup y$

b) $x * y = x \cap y$

c) $x * y = (x \cup y) - (x \cap y)$

**134.** Construa as tábuas das operações $*$ e $\triangle$ sobre $E = \{0, 1, 2, 3\}$ assim definidas:

a) $x * y =$ resto da divisão em $\mathbb{Z}$ de $x + y$ por 4

b) $x \triangle y =$ resto da divisão em $\mathbb{Z}$ de $x \cdot y$ por 4

**135.** Construa as tábuas das operações $\oplus$ e $\odot$ sobre $E = \{0, 1, 2, 3, 4\}$ assim definidas:

a) $x \oplus y =$ resto da divisão em $\mathbb{Z}$ de $x + y$ por 5

b) $x \odot y =$ resto da divisão em $\mathbb{Z}$ de $x \cdot y$ por 5

**136.** Construa a tábua da operação de reunião sobre a família de conjuntos $\mathcal{F} = \{A, B, C, D, E\}$ sabendo que $A \cup B = A$, $C \cup D = B$, $D \cup E = D$ e $E \cup C = C$.

**137.** Descreva pelas tábuas todas as operações sobre o conjunto $E = \{a, b\}$.

**138.** A partir da tábua ao lado, da operação $\triangle$ sobre $E = \{1, 2, 3, 4\}$, calcule os seguintes compostos:

a) $(3 \triangle 4) \triangle 2$

b) $3 \triangle (4 \triangle 2)$

c) $[4 \triangle (3 \triangle 3)] \triangle 4$

d) $(4 \triangle 3) \triangle (3 \triangle 4)$

e) $[(4 \triangle 3) \triangle 3] \triangle 4$

| △ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 3 | 4 |
| 3 | 1 | 3 | 4 | 2 |
| 4 | 1 | 4 | 2 | 3 |

**139.** Complete a tábua da operação $\circ$ (composição) definida sobre o conjunto de funções reais $E = \{f_1, f_2, f_3, f_4\}$, em que:

$f_1(x) = \frac{1}{x}$

$f_2(x) = -x$

$f_3(x) = -\frac{1}{x}$

$f_4(x) = x$

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | | | | |
| $f_2$ | | | | |
| $f_3$ | | | | |
| $f_4$ | | | | |

Depois responda:

a) Qual é o elemento neutro?

b) Que elementos têm simétrico?

c) Quais são os valores dos compostos $f_1^2, f_2^{-1}, f_3^3$ e $f_1^2 \circ f_2^{-1} \circ f_3^3$?

**140.** Construa a tábua da operação de composição sobre o conjunto de funções $E = \{f_1, f_2, f_3, f_4\}$, sabendo que essas funções são de $\mathbb{R}^2$ em $\mathbb{R}^2$, dadas por:

$f_1(x, y) = (x, y)$ $\qquad$ $f_3(x, y) = (x, -y)$

$f_2(x, y) = (-x, y)$ $\qquad$ $f_4(x, y) = (-x, -y)$

**141.** Seja $E = \{0, 1\}$. Seja $E^E$ o conjunto das aplicações de $E$ em $E$. Construa a tábua da operação de composição em $E^E$.

**142.** Construa a tábua da operação de composição de funções em $E = \{f_1, f_2, f_3, f_4\}$, em que:

$$f_1 = \{(a, a), (b, b), (c, c), (d, d)\} = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

$$f_2 = \{(a, b), (b, c), (c, d), (d, a)\} = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$$

$$f_3 = \{(a, c), (b, d), (c, a), (d, b)\} = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$$

$$f_4 = \{(a, d), (b, a), (c, b), (d, c)\} = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$$

Em seguida, calcule:

a) $f_2 \circ f_3 \circ f_4$

b) $f_3^2$

c) $(f_2 \circ f_4)^3$

d) $(f_3 \circ f_4)^{-1}$

e) $f_2^{-1}$

f) $f_2^{-1} \circ f_3^{-1}$

*Observação:* A notação $\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$, por exemplo, indica que a imagem de $a$ e $c$, de $b$ é $d$, de $c$ é $a$ e de $d$ é $b$.

**143.** Construa a tábua da operação de composição de funções em $E = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, em que:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

*Sugestão:* Observe no exercício 142 o significado dessa notação matricial.

**Como checar propriedades**

Vejamos agora como se pode checar uma a uma as propriedades de uma operação $*$ sobre $E = \{a_1, a_2, \dots, a_n\}$ quando $*$ é dada por meio de uma tábua.

**a) Propriedade associativa**

É aquela cuja verificação exige maior trabalho. A verificação pode ser feita de dois modos:

1º modo: Calculam-se todos os compostos do tipo $a_i * (a_j * a_k)$, com $i, j, k \in \{1, 2, \dots, n\}$; calculam-se todos os compostos do tipo $(a_i * a_j) * a_k$, com $i, j, k \in \{1, 2, \dots, n\}$; comparam-se os compostos que têm os mesmos $i$, $j$ e $k$. Como podemos notar, esse método requer o cálculo de $2n^3$ compostos.

2º modo: Encontra-se um conjunto $F$ dotado de uma operação $\triangle$ que se sabe ser associativa de tal forma que exista uma aplicação $f\colon E \to F$ com as seguintes propriedades:

a) $f$ é bijetora;

b) $f(x * y) = f(x) \triangle f(y)$ para todos $x, y \in E$.

Se isso ocorrer, a lei $*$ também é associativa, pois, para quaisquer $x, y, z \in E$, temos:

$$f((x*y)*z) = f(x*y) \triangle f(z) = (f(x) \triangle f(y)) \triangle f(z) =$$
$$= f(x) \triangle (f(y) \triangle f(z)) = f(x) \triangle f(y*z) = f(x*(y*z))$$

e, como $f$ é bijetora, vem: $(x*y)*z = x*(y*z)$

Você, estudante, poderá ter uma compreensão maior desse assunto quando estudar os isomorfismos (ver capítulo IV, seção IV.2).

**b) Propriedade comutativa**

Sabemos que uma operação $*$ é comutativa se $a_i * a_j = a_j * a_i$, ou seja, $a_{ij} = a_{ji}$, para quaisquer $i, j \in \{1, 2, 3, \dots, n\}$.

Chamando de diagonal principal da tábua da operação $*$ o conjunto formado pelos compostos $a_{11}, a_{22}, a_{33}, \dots, a_{nn}$, podemos notar que os compostos $a_{ij}$ e $a_{ji}$ ocupam posições simétricas relativamente à diagonal principal. Assim, uma operação $*$ é comutativa desde que sua tábua seja simétrica em relação à diagonal principal, isto é, compostos colocados simetricamente em relação à diagonal são iguais dois a dois.

Observe os quatro exemplos da página 125. Neles, as operações são comutativas.

Observe agora a tabela abaixo. É um exemplo de operação não comutativa. Note, por exemplo, que $b * c = a$ e $c * b = b$.

| $*$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $b$ | $a$ | $c$ |
| $b$ | $a$ | $b$ | $a$ |
| $c$ | $a$ | $b$ | $b$ |

**c) Elemento neutro**

Sabemos que um elemento $e$ é neutro para a operação $*$ quando:

(I) $e * a_j = a_j, \forall a_j \in E$

(II) $a_i * e = a_i$ e $\forall a_i \in E$

Da condição (I) decorre que a linha de $e$ é igual à linha fundamental. Da condição (II) decorre que a coluna de $e$ é igual à coluna fundamental.

Assim, uma operação $*$ tem neutro desde que exista um elemento cuja linha e coluna são respectivamente iguais à linha e coluna fundamentais.

Observe novamente os exemplos da página 125. Todos apresentam elemento neutro. Confira os neutros:

1º) 1; 2º) $A$ e $D$, respectivamente; 3º) 15; 4º) $f_1$.

Um exemplo de operação sem neutro é dado pela tábua abaixo. Notemos que $a$ é neutro só à esquerda (a linha de $a$ é igual à fundamental).

|   | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $c$ | $a$ | $b$ |
| $c$ | $b$ | $a$ | $c$ |

**d) Elementos simetrizáveis**

Sabemos que um elemento $a_i \in E$ é simetrizável para a operação $*$ que tem neutro e quando existe um $a_j \in E$ tal que:

(I) $a_i * a_j = e$

e

(II) $a_j * a_i = e$

Da condição (I) decorre que a linha de $a_i$ na tábua deve apresentar ao menos um composto igual a $e$.

Da condição (II) decorre que a coluna de $a_i$ deve apresentar ao menos um composto igual a $e$.

Como $a_{ij} = a_{ji} = e$, decorre que o neutro deve figurar em posições simétricas relativamente à diagonal principal.

Assim, um elemento $a_i$ é simetrizável quando o neutro figura ao menos uma vez na linha $i$ e na coluna $i$ da tábua, ocupando posições simétricas em relação à diagonal principal.

*Exemplos 36:*

1º) Neutro: $e$

Elementos simetrizáveis: $e, a, b, c$

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

2º) Neutro: $e$

Elementos simetrizáveis: $e, c, b$

| | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $d$ | $e$ | $c$ | $b$ |
| $c$ | $a$ | $e$ | $b$ | $d$ | $c$ |
| $d$ | $a$ | $d$ | $d$ | $d$ | $d$ |
| $e$ | $a$ | $b$ | $c$ | $d$ | $e$ |

**e) Elementos regulares**

Sabemos que um elemento $a \in E$ é regular em relação à operação $*$ quando:

(I) $a * a_i \neq a * a_j$, sempre que $a_i \neq a_j$

e

(II) $a_i * a \neq a_j * a$, sempre que $a_i \neq a_j$.

Isso significa que $a$ é regular quando, composto com elementos distintos de $E$, tanto à esquerda deles como à direita, produz resultados distintos.

Assim, um elemento $a$ é regular quando na linha e na coluna de $a$ não há elementos iguais.

*Exemplos 37:*

Os elementos regulares são $e, a, d$.

Note que na linha e coluna de $b$ ocorrem repetições. Nas de $c$, também.

| | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ |
| $b$ | $b$ | $c$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $d$ | $c$ | $a$ | $b$ |
| $d$ | $d$ | $e$ | $a$ | $b$ | $c$ |

## Exercícios

**144.** A partir das tábuas construídas no exercício 132, responda:

a) Que operações são comutativas?

b) Que operações apresentam elemento neutro?

c) Quais são os elementos simetrizáveis?

d) Quais são os elementos regulares?

**145.** A tábua abaixo descreve a operação *não associativa* $\triangle$ sobre o conjunto $E = \{a, b, c, d\}$. Calcule de cinco formas diferentes o composto $a \triangle b \triangle c \triangle d$, ou seja:

a) $(a \triangle b) \triangle (c \triangle d)$

b) $[a \triangle (b \triangle c)] \triangle d$

c) $[(a \triangle b) \triangle c] \triangle d$

d) $a \triangle [(b \triangle c) \triangle d]$

e) $a \triangle [b \triangle (c \triangle d)]$

| $\triangle$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $b$ | $b$ | $c$ | $d$ |
| $b$ | $c$ | $d$ | $d$ | $a$ |
| $c$ | $d$ | $d$ | $a$ | $b$ |
| $d$ | $a$ | $b$ | $b$ | $c$ |

**146.** Construa a tábua da operação de interseção sobre a família de conjuntos $\mathcal{F} = \{A, B, C, D\}$, sabendo que:

$$A \cap B = B, B \cap C = C \text{ e } C \cap D = D$$

Em seguida, estabeleça:

a) qual é o elemento neutro;

b) que elementos são simetrizáveis;

c) que elementos são regulares.

**147.** A partir de cada tábua abaixo, decida:

i) A operação é comutativa?

ii) Existe elemento neutro?

iii) Que elementos são simetrizáveis?

iv) Que elementos são regulares?

a)

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $c$ | $d$ | $a$ | $b$ |
| $b$ | $d$ | $c$ | $b$ | $a$ |
| $c$ | $a$ | $b$ | $c$ | $d$ |
| $d$ | $b$ | $a$ | $d$ | $c$ |

b)

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $c$ | $a$ | $d$ | $b$ |
| $b$ | $a$ | $b$ | $c$ | $d$ |
| $c$ | $b$ | $c$ | $d$ | $a$ |
| $d$ | $d$ | $d$ | $a$ | $c$ |

c)

| | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
|---|---|---|---|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
| $b$ | $b$ | $c$ | $d$ | $a$ | $f$ | $g$ | $h$ | $e$ |
| $c$ | $c$ | $d$ | $a$ | $b$ | $g$ | $h$ | $e$ | $f$ |
| $d$ | $d$ | $a$ | $b$ | $c$ | $h$ | $e$ | $f$ | $g$ |
| $e$ | $e$ | $f$ | $g$ | $h$ | $a$ | $b$ | $c$ | $d$ |
| $f$ | $f$ | $g$ | $h$ | $e$ | $b$ | $c$ | $d$ | $a$ |
| $g$ | $g$ | $h$ | $e$ | $f$ | $c$ | $d$ | $a$ | $b$ |
| $h$ | $h$ | $e$ | $f$ | $g$ | $d$ | $a$ | $b$ | $c$ |

**148.** Complete a tábua da operação $*$ sobre o conjunto $E \quad \{a, b, c, d\}$, sabendo que:

(I) $b$ é o elemento neutro

(II) o simétrico de $a$ é $a$

(III) o simétrico de $c$ é $d$

(IV) $a * c = d$

(V) todos os elementos de $E$ são regulares

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | | | | |
| $b$ | | | | |
| $c$ | | | | |
| $d$ | | | | |

**149.** Construa a tábua de uma operação $*$ sobre $E = \{e, a, b, c\}$ de modo a satisfazer às seguintes condições:

(I) $*$ seja comutativa

(II) $e$ seja o elemento neutro

(III) $x * a = a, \forall x$

(IV) $R_*(E) = E - \{a\}$

**150.** Construa a tábua de uma operação $*$ sobre o conjunto $E = \{a, b, c, d\}$ de modo que satisfaça às condições seguintes:

(I) seja comutativa

(II) $a$ seja o elemento neutro

(III) $U_*(E) \quad E$

(IV) $R_*(E) - E$

(V) $b * c = a$

**151.** Complete a tábua da operação $*$ sobre o conjunto $E = \{a, b, c, d, e\}$, sabendo que:

(I) $e * x = x = x * e, \forall x$

(II) $a * x = a = x * a, \forall x$

(III) $x * x = e, \forall x \neq a$

(IV) $b * d = c$

(V) $b, c, d$ são regulares

| $*$ | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| $a$ | | | | | |
| $b$ | | | | | |
| $c$ | | | | | |
| $d$ | | | | | |
| $e$ | | | | | |

**152.** Seja $*$ a operação sobre $E \quad \{1, 2, 3, 4, 6, 12\}$ dada pela lei $x * y \quad \text{mmc}(x, y)$. Determine os subconjuntos de $E$ que têm três elementos e são fechados em relação a essa operação.

**153.** Seja $E = \mathcal{P}\{a, b, c\}$. Qual é a condição sobre $X$ e $Y$, sendo $X \in E$ e $Y \in E$, para que $\{X, Y\}$ seja fechado em relação à operação de interseção sobre $E$?

**154.** Dê um exemplo de operação não associativa nem comutativa, mas que tem elemento neutro.

**155.** Dê um exemplo de operação sobre $E$ (finito) em que todo elemento de $E$ é regular, existe elemento neutro e só ele é simetrizável.

**156.** Dê um exemplo de operação em que o composto de dois elementos simetrizáveis não é simetrizável.

**157.** Dê um exemplo de operação sobre $E$ (finito) em que existe elemento neutro e todos os elementos de $E$, com exceção do neutro, têm dois simétricos.

## Exercícios complementares

**C18.** a) Prove que o número de operações, duas a duas distintas, sobre um conjunto finito e não vazio com $n$ elementos é $n^{(n)^2}$.

b) Prove que o número de operações comutativas, duas a duas distintas, sobre um conjunto finito e não vazio com $n$ elementos é $\left(\frac{n^2 + n}{2}\right)$ expoente de $n$.

**C19.** Seja $E$ um conjunto munido de uma operação $*$ que apresenta um elemento neutro e. Prove que $*$ é associativa e comutativa se, e somente se, $a * (b * c) = (a * c) * b$, quaisquer que sejam $a, b, c \in E$.

**C20.** Uma operação $*$ sobre um conjunto $E$ é dita totalmente não associativa se

$$(a * b) * c \neq a * (b * c)$$

quaisquer que sejam $a, b, c \in E$.

a) Mostre que tal operação não é comutativa.

b) Mostre que a operação de potenciação ($x * y = x^y$) sobre $E = \{3, 4, \ldots\}$ é totalmente não associativa.

**C21.** Seja $*$ uma operação sobre $E$ que é associativa e tem neutro. Sendo $A$ um subconjunto não vazio de $E$, indiquemos com $C(A)$ o conjunto dos elementos $x \in E$ tais que $a * x = x * a$ para todo $a \in A$.

Prove que.

a) $C(A)$ é fechado para a operação $*$.

b) Se $B \subset A$, entao $C(B) \supset C(A)$.

c) $C(C(C(A)))$ $C(A)$

## 18. OPERAÇÕES EM $\mathbb{Z}_m$

Vamos definir aqui as operações de adição e multiplicação num conjunto $\mathbb{Z}_m$ ($m > 1$) de classes de restos. Em seguida mostraremos algumas propriedades dessas operações.

**Definição 45:** Dadas duas classes $\bar{a}, \bar{b} \in \mathbb{Z}_m$, chama-se soma $\bar{a} + \bar{b}$ a classe $\overline{a+b}$.

**Definição 46:** Dadas duas classes $\bar{a}, \bar{b} \in \mathbb{Z}_m$, chama-se produto $\bar{a} \cdot \bar{b}$ a classe $\overline{a \cdot b}$.

**Observação**

Se $\bar{a} = \overline{a'} \in \mathbb{Z}_m$ e $\bar{b} = \overline{b'} \in \mathbb{Z}_m$, então $a \equiv a'$ (mod $m$) e $b \equiv b'$ (mod $m$); portanto, $a + b \equiv a' + b'$ (mod $m$) e $a \cdot b \equiv a' \cdot b'$ (mod $m$) e, conseqüentemente, $\overline{a+b} = \overline{a'+b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$. Isso mostra que a soma e o produto de classes, conforme as definições 45 e 46, não dependem dos representantes das classes. Dessa forma fica garantido que $\overline{a+b}$ é única e $\overline{a \cdot b}$ também é única, ou seja, as aplicações $(\bar{a}, \bar{b}) \mapsto \overline{a+b}$ e $(\bar{a}, \bar{b}) \mapsto \overline{a \cdot b}$ são operações sobre $\mathbb{Z}_m$, denominadas *adição* e *multiplicação*, respectivamente.

**Propriedades da adição**

1) *Associativa*

Para quaisquer $a, b, c \in \mathbb{Z}_m$, temos:

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c} = \overline{a+(b+c)} = \\ = \overline{(a+b)+c} = \overline{a+b} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$$

2) *Comutativa*

Para quaisquer $\bar{a}, \bar{b} \in \mathbb{Z}_m$, temos:

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

3) *Elemento neutro*

Para qualquer $\bar{a} \in \mathbb{Z}_m$, temos:

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$$

Portanto, $\bar{0}$ é o neutro da adição em $\mathbb{Z}_m$.

4) *Elementos simetrizáveis*

Dado $\bar{a} \in \mathbb{Z}_m$, procuremos seu simétrico $\overline{a'}$.

Devemos ter $\bar{a} + \overline{a'} = \overline{a+a'} = \bar{0}$ e, portanto, $a + a' \equiv 0$ (mod $m$) ou $a' \equiv -a$ (mod $m$). De onde, $\overline{a'} = \overline{m-a}$.

Isso mostra que todo elemento $\bar{a} \in \mathbb{Z}_m$ é simetrizável para a adição e seu simétrico é $\overline{m-a}$.

**Propriedades da multiplicação**

Analogamente, pode se provar a associativa e a comutativa.

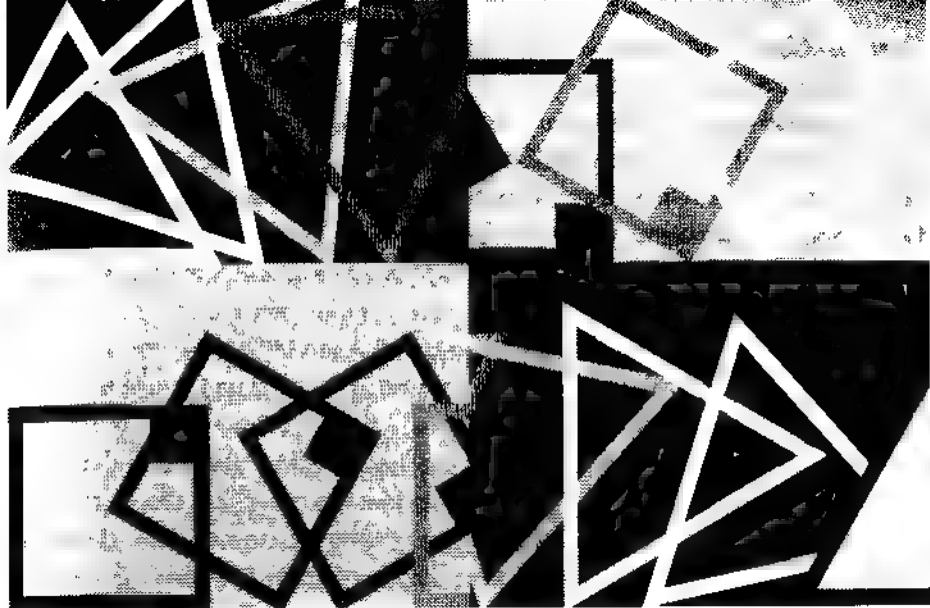
Para qualquer $\overline{a} \in \mathbb{Z}_m$, temos:

$$a \cdot 1 - a \cdot 1 = \dot{a}$$

Portanto, $\overline{1}$ é o neutro da multiplicação em $\mathbb{Z}_m$.

Provaremos que $\overline{a} \in \mathbb{Z}_m$ é simetrizável para a multiplicação se, e somente se, mdc$(a, m) = 1$.

($\rightarrow$) Seja $a \in \mathbb{Z}_m$ um elemento inversível. Existe, então, $\overline{a'} \in \mathbb{Z}_m$ tal que $a \cdot a' = \cdot\, a \cdot \overline{a}' - 1$ Daí, $aa' - 1 \pmod{m}$ ou $aa' \quad 1 \quad mq$, para algum $q \in \mathbb{Z}$. A proposição 2, do capítulo II, garante então que mdc$(a, m) - 1$.

($\leftarrow$) Se mdc$(a, m) = 1$, então, devido à mencionada proposição, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = 1$. Dessa igualdade segue que $ax_0 - 1 = m(-y_0)$ e, portanto, que $ax_0 \equiv 1 \pmod{m}$. De onde, $\overline{ax_0} = \overline{1}$ ou $\overline{a} \cdot \overline{x_0} = \overline{1}$, igualdade que mostra que $\overline{a}$ é inversível e $\overline{x_0}$ é seu inverso.

CAPÍTULO IV

# GRUPOS

## IV-1 GRUPOS E SUBGRUPOS

### 1. NOTA HISTÓRICA

Entre 1500 e 1515, o matemático italiano Scipione del Ferro (1456-1526) descobriu um procedimento para resolver a equação cúbica $x^3 + px = q$ $(p, q > 0)$ (em notação atual). Esse procedimento se traduz, modernamente, na seguinte fórmula:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} - \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$$

Del Ferro mostrou, com isso, que é possível expressar as raízes da cúbica considerada em termos de seus coeficientes, usando apenas *adições*, *subtrações*, *multiplicações*, *divisões* e *radiciações*. Ou, como se diz modernamente, que a equação dada é *resolúvel por radicais*.

Como já se sabia há muitos séculos que as equações de grau um e dois também são resolúveis por radicais (no caso destas últimas, lembrar a chamada fórmula de Bhaskara), a solução de del Ferro colocou o seguinte desafio para os algebristas: será que toda equação algébrica é resoluvel por radicais? As pesquisas visando responder a essa questão se arrastaram por mais de dois séculos e meio, frustraram alguns dos grandes matemáticos desse período e contribuíram decisivamente para a criação do conceito de "grupo".

Na verdade a questão da resolubilidade das equações algébricas só começou a ser esclarecida genericamente na segunda metade do século XVIII. Na obra *Réflexions sur la resolution algébrique des équations* (Reflexões sobre a resolução algébrica de equações) (1770-1771), o ítalo-francês Joseph-Louis Lagrange (1736-1813), possivelmente o primeiro matemático a perceber com lucidez maior o caminho a ser seguido para abordar o problema, observou que a "teoria das permutações" era de grande importância para a resolução de equações. Lagrange referia-se a permutações envolvendo as raízes da equação.

Em 1824, o matemático norueguês Niels Henrik Abel (1802-1829) provaria aquilo de que Lagrange suspeitara fortemente: que não há nenhuma fórmula geral por radicais para resolver as equações de grau $\geqslant 5$.

Ainda assim uma questão permanecia em pé: já que as equações de grau $\geqslant 5$ não são, de modo geral, resolúveis por radicais, mas alguns tipos o são, como já se sabia bem antes de Abel, o que caracteriza matematicamente estas últimas? A resposta a essa pergunta seria dada pelo matemático francês Evariste Galois (1811-1832), em cuja obra aparece delineado pela primeira vez o conceito de grupo, inclusive com esse nome. Resumidamente, a idéia de Galois para responder a essa pergunta foi associar a cada equação um grupo formado por permutações de suas raízes e condicionar a resolubilidade por radicais a uma propriedade desse grupo. E, como para toda equação de grau $\leqslant 4$ o grupo de permutações que lhe é associado goza dessa propriedade e para $n > 4$ sempre há equações cujo grupo não se sujeita a essa propriedade, a questão da resolubilidade por radicais estava por fim esclarecida.

Com o tempo, verificou-se que a idéia de grupo era um instrumento da mais alta importância para a organização e o estudo de muitas partes da matemática. Em nível mais elementar, um exemplo é a teoria das simetrias, muito importante para a cristalografia e a química, por exemplo. Essencialmente, os grupos podem ser usados para retratar simetrias geométricas: a cada figura associa-se um grupo, grupo esse que caracteriza e retrata a simetria da figura. Em **2.4** (xiii-a e xiii-b) discorreremos um pouco sobre isso.

## 2. GRUPOS E SUBGRUPOS

### 2.1 Conceito de grupo

**Definição 1:** Um sistema matemático constituído de um conjunto não vazio $G$ e uma operação $(x, y) \mapsto x * y$ sobre $G$ é chamado *grupo* se essa operação se sujeita aos seguintes axiomas:

*associatividade*

$(a * b) * c = a * (b * c)$, quaisquer que sejam $a, b, c \in G$;

*existência de elemento neutro*

existe um elemento $e \in G$ tal que $a * e = e * a = a$, qualquer que seja $a \in G$;

*existência de simétricos*

para todo $a \in G$ existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$.

Se, além disso, ainda se cumprir o axioma da

*comutatividade*

$a * b = b * a$, quaisquer que sejam $a, b \in G$,

o grupo recebe o nome de *grupo comutativo* ou *abeliano*.

Mantidas as notações da definição, um grupo poderá ser indicado apenas por $(G, *)$, em que, para facilitar, o símbolo $*$ indica a operação sobre $G$. E, quando não houver possibilidade de confusão, até esse símbolo poderá ser omitido. Assim, será comum usarmos expressões como, por exemplo, "Seja $G$ um grupo" ou "Consideremos um grupo $G$", o que naturalmente pressupõe a operação subentendida. Outra maneira ainda de nos referirmos a um grupo $(G, *)$ é dizer que "$G$ tem uma estrutura de grupo em relação à operação $*$".

## 2.2 Propriedades imediatas de um grupo

Seja $(G, *)$ um grupo. As propriedades já demonstradas para uma operação sobre um conjunto (capítulo III) nos asseguram:

- a unicidade do elemento neutro de $(G, *)$;
- a unicidade do simétrico de cada elemento de $G$;
- que, se $e$ é o elemento neutro, então $e' = e$;
- que $(a')' = a$, qualquer que seja $a \in G$;
- que $(a * b)' = b' * a'$ e, portanto (raciocinando por indução), que $(a_1 * a_2 * \ldots * a_n)' = a_n' * a_{n-1}' * \ldots * a_1'$ $(n \geqslant 1)$;
- que todo elemento de $G$ é regular para a operação $*$. Ou seja: se $a * x = a * y$ (ou $x * a = y * a$), então $x = y$.

Além disso, pode-se demonstrar também que

- no grupo $G$, a equação $a * x = b$ $(x * a = b)$ tem conjunto solução unitário, constituído do elemento $a' * b$ (respectivamente, $b * a'$).

Consideremos $a * x = b$. Substituindo-se $x$ por $a' * b$ no primeiro membro da equação, obtém-se

$$a * (a' * b) = (a * a') * b = e * b = b$$

o que garante que efetivamente $a' * b$ é solução da equação. Por outro lado, se $x_0$ é uma solução, então $a * x_0 = b$. Daí:

$$a' * (a * x_0) = a' * b$$

Como $a' * (a * x_0) = (a' * a) * x_0 = x_0$, então $x_0 = a' * b$.

Nesta altura, cabem algumas observações no que diz respeito à linguagem a ser empregada daqui para a frente:

(i) Um grupo cuja operação é uma "adição" será chamado de *grupo aditivo*, ao passo que, se a operação é uma "multiplicação", de *grupo multiplicativo*. No caso de grupo aditivo, o simétrico de um elemento $a$ é chamado *oposto* de $a$ e indicado por $-a$; e, no caso de um grupo multiplicativo, *inverso* de $a$ e denotado por $a^{-1}$.

(ii) Na maior parte da teoria sobre grupos a ser desenvolvida aqui usaremos a notação multiplicativa para indicar a operação. Motivo: é mais prática e, é claro, os resultados obtidos valem em qualquer caso, bastando mudar convenientemente a notação.

## 2.3 Grupos finitos

Um grupo $(G, *)$ em que o conjunto $G$ é finito, chama-se *grupo finito*. Nesse caso, o número de elementos de $G$ é chamado *ordem* do grupo (notação $o(G)$) e a tábua da operação $*$ se denomina *tábua do grupo*. Diga-se de passagem que o primeiro matemático a usar tábuas para representar grupos foi o inglês Arthur Cayley (1821–1899). Cayley, que valorizava sobremodo os aspectos formais da matemática, foi provavelmente o precursor do estudo abstrato da teoria dos grupos. Outra realização importante desse matemático foi a introdução das matrizes na matemática.

*Exemplo 1:* É fácil verificar que $G = \{-1, +1\}$ é um grupo multiplicativo. Sua ordem obviamente é 2 e sua tábua:

| $\cdot$ | 1 | −1 |
|---|---|---|
| 1 | 1 | −1 |
| −1 | −1 | 1 |

## 2.4 Alguns grupos importantes

(i) *Grupo aditivo dos inteiros (comutativo)*

Sistema formado pelo conjunto dos inteiros e a adição usual sobre esse conjunto. Motivo: a adição usual é uma operação sobre $\mathbb{Z}$, associativa e comutativa. Mais: há um elemento neutro para ela (o número 0), e o oposto $-a$ de um elemento $a \in \mathbb{Z}$ também pertence a esse conjunto. Obviamente essas propriedades são pré-requisitos para este trabalho.

(ii) *Grupo aditivo dos racionais (comutativo)*

Sistema formado por $\mathbb{Q}$ e a adição usual sobre esse conjunto. O porquê é o mesmo do exemplo anterior.

(iii) *Grupo aditivo dos reais (comutativo)*

Sistema formado por $\mathbb{R}$ e a adição usual sobre esse conjunto. O porquê é o mesmo do primeiro exemplo.

(iv) *Grupo aditivo dos complexos (comutativo)*

A *soma* de dois números complexos $z = a + bi$ e $w = c + di$ é definida por $z + w = (a + b) + (c + d)i$. É fácil verificar que essa operação é associativa. Mais ainda verificar que $0 = 0 + 0 \cdot i$ é elemento neutro dessa operação. Por fim, para todo complexo $z = a + bi$, o número complexo $-z = (-a) + (-b)i$ é seu oposto, o que pode ser verificado diretamente sem nenhuma dificuldade.

(v) *Grupo multiplicativo dos racionais (comutativo)*

Sistema formado pelo conjunto dos racionais não nulos e a multiplicação usual sobre esse conjunto. O conjunto $\mathbb{Q}^*$ é fechado em relação à multiplicação, ou seja, o produto de dois números racionais não nulos também é diferente de zero. A multiplicação usual é associativa em $\mathbb{Q}^*$ porque o é em $\mathbb{Q}$; o número 1, elemento neutro da multiplicação, obviamente é diferente de 0; e se $a \neq 0$, o mesmo acontece com seu inverso $a^{-1}$. Também neste caso admitimos como pré-requisito o conhecimento das propriedades da multiplicação de números racionais.

*Contra-exemplo 1:* O sistema formado pelo conjunto $\mathbb{Z}^*$ e a multiplicação de números inteiros não é um grupo, embora o produto de dois inteiros não nulos seja sempre um inteiro não nulo. Ocorre que nenhum inteiro $a$, salvo 1 e $-1$, tem inverso em $\mathbb{Z}$.

(vi) *Grupo multiplicativo dos reais (comutativo)*

Sistema formado por $\mathbb{R}^*$ e a multiplicação usual sobre esse conjunto. O porquê é o mesmo do exemplo anterior.

(vii) *Grupo multiplicativo dos complexos (comutativo)*

Sistema formado pelo conjunto $\mathbb{C}^*$ e a multiplicação usual de números complexos. O produto de dois números complexos $z = a + bi$ e $w = c + di$ é definido por $zw = (ac - bd) + (ad + bc)i$. Se os números dados são diferentes de 0, o mesmo acontece com o produto, como se pode verificar. Essa operação é associativa e comutativa, e a verificação disso é apenas uma questão de cálculos algébricos; o elemento neutro é $1 = 1 + 0i$, e o inverso de um elemento $z = a + bi$, não nulo, é $z^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i$, também um número complexo não nulo, considerando-se que $a \neq 0$ ou $b \neq 0$.

(viii) *Grupo aditivo de matrizes* m × n *(comutativo)*

Nas considerações a serem feitas aqui indicaremos por $K$, indistintamente, um dos seguintes conjuntos, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, e por $M_{m \times n}(K)$ o conjunto das matrizes sobre $K$ com $m$ linhas e $n$ colunas. Isso posto mostraremos que $M_{m \times n}(K)$ é um grupo aditivo. Para isso, lembremos primeiro que a adição de matrizes em $M_{m \times n}(K)$ é definida da seguinte maneira:

Se

$$A \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad \text{e} \quad B \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$$

então

$$A + B = \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

e, portanto, trata se de uma operação sobre o conjunto $M_{m \times n}(K)$

Essa adição cumpre os axiomas exigidos pela definição 1, o que é fácil de provar:

*Associatividade:* $A + (B + C) = (A + B) + C$

*Comutatividade:* $A + B = B + A$

*Existência de elemento neutro:* é a matriz

$$O_{m \times n} = \begin{pmatrix} 0 & \dots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \dots & 0 \end{pmatrix}$$

*Existência de opostos:* qualquer que seja a matriz

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

tomando-se

$$-A = \begin{pmatrix} -a_{11} & \dots & -a_{1n} \\ \cdots & \cdots & \cdots \\ -a_{m1} & \dots & -a_{mn} \end{pmatrix}$$

que obviamente também é uma matriz de $M_{m \times n}(K)$, então:

$$A + (-A) = \begin{pmatrix} a_{11} - a_{11} & \dots & a_{1n} - a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} - a_{m1} & \dots & a_{mn} - a_{mn} \end{pmatrix} = O_{m \times n}$$

Portanto, $(M_{m \times n}(K), +)$ é um grupo aditivo abeliano quando $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

(ix) *Grupos lineares de grau n (multiplicativo, não comutativo se n* $> 1$)

Indicaremos agora por $K$, indistintamente, um dos conjuntos $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ e por $M_n(K)$ o conjunto das matrizes de ordem $n$ sobre $K$. Tratando-se de um caso particular do exemplo anterior, $M_n(K)$ é um grupo aditivo. No que se refere à multiplicação de matrizes, porém, a situação é diferente. Lembremos que a multiplicação de matrizes (linhas por colunas) é definida da seguinte maneira: se $A = (a_{ij})$ e $B = (b_{ij})$, então:

$$AB = (c_{ij}), \text{ em que } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \ (i, j = 1, 2, \dots, n)$$

Para essa operação vale a associatividade, como é bem conhecido. Mais: ela conta com um elemento neutro que é a matriz idêntica de ordem $n$:

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Mas sempre há matrizes para as quais não há a matriz inversa por exemplo, a matriz nula

$$O_n = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

cujo produto por uma matriz qualquer é ela mesma, portanto diferente de $I_n$.

Para saber quais matrizes de ordem $n$ têm inversa, recorremos ao seguinte teorema da teoria dos determinantes: "Uma matriz $A \in M_n(K)$ é inversível se, e somente se, $det(A) \neq 0$". Como o conjunto das matrizes inversíveis, que indicaremos por $GL_n(K)$, inclui a matriz idêntica $I_n$, cujo determinante é igual a 1 e $\det(AB) = \det(A)\det(B) \neq$ $\neq 0, \forall A, B \in GL_n(K)$, então $(GL_n(K), \cdot)$ é um grupo. Esse grupo não é comutativo quando $n > 1$, pois, por exemplo, se

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \text{ e } B = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

então.

$$AB = \begin{pmatrix} n & \dots & 1 \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ 1 & \dots & 1 \end{pmatrix} \text{ e } BA = \begin{pmatrix} 1 & \dots & 1 \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ 1 & \dots & n \end{pmatrix}$$

O grupo $(GL_n(K), \cdot)$ é chamado, respectivamente, *grupo linear racional*, *real* ou *complexo, de grau* n, conforme $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$

(x) *Grupos aditivos de classes de restos (comutativo)*

Lembremos que, para qualquer inteiro $m > 1$, o conjunto das classes de resto módulo $m$, ou seja, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$ é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência, módulo $m$. Portanto, $\overline{0}$ é formado por todos os inteiros côngruos a 0, módulo $m$, $\overline{1}$ por todos os inteiros côngruos a 1, módulo $m$, e assim por diante. No capítulo anterior vimos que a adição módulo $m$, definida por

$$\overline{a} + \overline{b} = \overline{a+b}$$

é uma operação sobre $\mathbb{Z}_m$ para a qual vale a associatividade e a comutatividade. E que, além disso:

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$$

e, portanto, $\overline{0}$ é o elemento neutro dessa operação. Mais, que a classe $\overline{m-a}$ é o oposto de $\overline{a} \in \mathbb{Z}_m$ na adição módulo $m$, pois

$$\overline{a} + \overline{m-a} = \overline{a+(m-a)} = \overline{m} = \overline{0}$$

uma vez que $m \equiv 0 \pmod m$. Então $-\overline{a} = \overline{m-a}$

De onde $(\mathbb{Z}_m, +)$ é um grupo comutativo, para todo inteiro $m > 1$, chamado *grupo aditivo das classes de resto módulo* m. Vale notar que a ordem desse grupo e $m$

*Exemplo 2:* Construir a tábua do grupo $(\mathbb{Z}_3, +)$.

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

(xi) *Grupos multiplicativos de classes de restos*

No capítulo anterior, vimos também como se introduz a multiplicação módulo $m$ em $\mathbb{Z}_m$:

se $\bar{a}, \bar{b} \in \mathbb{Z}_m$, então $\bar{a} \cdot \bar{b} = \overline{ab}$.

Naquela oportunidade mostramos que essa operação está bem definida e goza das propriedades associativa e comutativa; além disso, a classe $\bar{1}$ é o elemento neutro, uma vez que $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}$.

Mas ocorre que, mesmo excluindo-se o elemento $\bar{0}$ de $\mathbb{Z}_m$, que obviamente não tem inverso para a multiplicação módulo $m$, nem sempre o conjunto restante é um grupo multiplicativo. De fato, a restrição da multiplicação módulo 4 aos elementos de $\mathbb{Z}_4 - \{\bar{0}\}$, por exemplo, nem sequer é uma operação sobre esse conjunto, uma vez que $\bar{2} \cdot \bar{2} = \bar{0}$.

Provaremos agora que a restrição da multiplicação módulo $m$ aos elementos de $\mathbb{Z}_m^* = \mathbb{Z}_m - \{\bar{0}\}$ é uma operação sobre esse conjunto se, e somente se, $m$ é um número primo.

$(\rightarrow)$ Suponhamos que $m$ não fosse primo. Como $m > 1$, podem ser encontrados dois inteiros $a, b > 1$ tais que $ab = m$. Dessa igualdade resulta que $\overline{ab} = \bar{m}$. Como $\bar{a} \cdot \bar{b} = \overline{ab}$ e $\bar{m} = \bar{0}$, então $\bar{a} \cdot \bar{b} = \bar{0}$, o que é impossível em face da hipótese.

$(\leftarrow)$ A única possibilidade de a multiplicação módulo $m$, quando restrita aos elementos de $\mathbb{Z}_m^*$, não ser uma operação sobre esse conjunto é acontecer de $\overline{a \cdot b} = \bar{0}$ para algum par de elementos desse conjunto. Mas isso implicaria $\overline{ab} = \bar{0}$ e, portanto, $ab \equiv 0 \pmod{m}$. Daí, $m \mid ab$ e, como $m$ é primo por hipótese, então $m \mid a$ ou $m \mid b$. Considerando-se, por exemplo, a primeira hipótese, $a = mq$, para algum inteiro $q$, e, portanto:

$$\bar{a} = \overline{mq} = \bar{m} \cdot \bar{q} = \bar{0} \cdot \bar{q} = \bar{0}$$

o que é um absurdo, visto que, por hipótese, $\bar{a} \in \mathbb{Z}_m^*$.

Mostraremos agora que, se $m$ é primo, a multiplicação módulo $m$, quando restrita aos elementos de $\mathbb{Z}_m^*$, faz desse conjunto um grupo. Para isso basta mostrar que, qualquer que seja o elemento $\bar{a} \in \mathbb{Z}_m^*$, pode-se encontrar $\bar{b} \in \mathbb{Z}_m^*$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$.

De fato, se $\overline{a} \in \mathbb{Z}_m^*$, então $a$ não é múltiplo de $m$. E, como $m$ é primo, então $\text{mdc}(m, a) = 1$. Daí, $mx_0 + ay_0 = 1$, para convenientes inteiros $x_0$ e $y_0$ (identidade de Bezout). Reduzindo-se essa igualdade, módulo $m$,

$$\overline{mx_0 + ay_0} = \overline{m} \cdot \overline{x_0} + \overline{a} \cdot \overline{y_0} = \overline{a} \cdot \overline{y_0} = \overline{1}$$

o que mostra que $\overline{y_0}$ (que pertence a $\mathbb{Z}_m^*$) é o inverso de $\overline{a}$.

As considerações anteriores permitem concluir que $\mathbb{Z}_m^*$ é um grupo multiplicativo se, e somente se, $m$ é primo.

*Exemplo 3.* Determinemos o inverso de 4 em $\mathbb{Z}_5^*$, usando o raciocínio da última demonstração. Ora, uma solução de $5x_0 + 4y_0 = 1$, que pode ser determinada por simples observação, é $(1, -1)$. Logo, $y_0 = -1$ e, portanto, o inverso de $\overline{4}$ é $\overline{-1} = \overline{4}$, pois $4 \equiv -1 \pmod 5$.

(xii) *Grupos de permutações*

(xii-a) *Permutação* é o termo específico usado na teoria dos grupos para designar uma bijeção de um conjunto nele mesmo. Se $E$ indica um conjunto não vazio, denotaremos por $S(E)$ o conjunto das permutações dos elementos de $E$. A composição de aplicações é, neste caso, uma operação sobre $S(E)$, pois, se $f$ e $g$ são permutações de $E$, ou seja, se $f: E \to E$ e $g: E \to E$ são bijeções, então a composta $g \circ f: E \to E$ também é uma bijeção, como vimos no capítulo anterior.

Vimos também que vale a associatividade para essa operação e que $i_E: E \to E$ (aplicação idêntica de $E$), que obviamente é uma bijeção, é o elemento neutro nesse caso, posto que: $(i_E \circ f)(x) = i_E(f(x)) = f(x)$, para todo $x \in E$, o que garante a igualdade $i_E \circ f = f$. Analogamente se prova que $f \circ i_E = f$. Finalmente, se $f$ é uma permutação de $E$, então o mesmo acontece com $f^{-1}$ (aplicação inversa de $f$), que, como também foi visto no capítulo anterior, é uma bijeção e é o elemento inverso de $f$ para a composição de aplicações, pois $f \circ f^{-1} = f^{-1} \circ f = i_E$.

Portanto, $(S(E), \circ)$ é um grupo — *o grupo das permutações sobre* E. Esse grupo é comutativo se, e somente se, sua ordem é 1 ou 2. De fato, se a ordem é 1, $S(E)$ só possui um elemento, a aplicação idêntica que, naturalmente, comuta consigo mesma. Se a ordem é 2 e os elementos de $E$ forem indicados por $a$ e $b$, então $S(E)$ também só tem dois elementos: a aplicação idêntica e a aplicação que leva $a$ em $b$, e vice-versa. Como, obviamente, esta última aplicação comuta consigo mesma e com $i_E$, então $(S(E), \circ)$ também é comutativo nesse caso.

Suponhamos agora que $o(S(E)) > 2$ e que, portanto, $E$ tenha mais do que 2 elementos. Designando por $a$, $b$ e $c$ três elementos distintos de $E$, consideremos as permutações $f$ e $g$ de $S(E)$ definidas da seguinte maneira:

$f(a) = b$, $f(b) = a$ e $f(x) = x$ qualquer que seja $x \neq a, b$

e

$g(a) = c$, $g(c) = a$ e $g(x) = x$ qualquer que seja $x \neq a, c$.

É claro que $f$ e $g$ sao permutações de $E$, pela maneira como foram construídas. Alem disso,

$$(f \circ g)(a) = f(g(a)) = f(c) = c$$

e

$$(g \circ f)(a) = g(f(a)) = g(b) = b,$$

o que mostra que $g \circ f \neq f \circ g$ e, portanto, que $S(E)$ não é comutativo.

(xii-b) Um caso particular importante de grupo de permutações, aliás relacionado com a origem da teoria dos grupos (ver **Nota Histórica** deste capítulo), é aquele em que $E = \{1, 2, \dots, n\}$, em que $n \geqslant 1$. Neste caso, em vez da notação genérica $S(E)$, usa-se $S_n$ para indicar o conjunto das permutações sobre $E$. E o próprio grupo $(S_n, \circ)$ tem um nome especial: *grupo simétrico de grau* n. A análise combinatória nos ensina que esse grupo tem ordem $n!$, número de permutações que se podem construir com $n$ elementos, permutações essas que podem naturalmente ser colocadas em correspondência biunívoca com os elementos de $S_n$.

Para o estudo dos grupos simétricos costuma-se usar a seguinte notação: se $f \in S_n$ e $f(1) = i_1, f(2) = i_2, \dots, f(n) = i_n$, então:

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

Por exemplo, a permutação idêntica é denotada por

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Nessa notação, a ordem das colunas não importa, embora em geral se usem os elementos da primeira linha em ordem crescente. Por exemplo, em $S_3$,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

pois ambas têm o mesmo efeito sobre os elementos de $E$.

Com essa notação, a composição de duas permutações

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \quad \text{e} \quad g = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

se faz da seguinte maneira:

$$g \circ f = \begin{pmatrix} 1 & \dots & i_r & \dots & n \\ j_1 & \dots & j_{i_r} & \dots & j_n \end{pmatrix} \circ \begin{pmatrix} 1 & \dots & r & \dots & n \\ i_1 & \dots & i_r & \dots & i_n \end{pmatrix} = \begin{pmatrix} \dots & r & \dots \\ \dots & j_{i_r} & \dots \end{pmatrix}$$

pois $(g \circ f)(r) = g(f(r)) = g(i_r) = j_{i_r}$

Por exemplo, em $S_4$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Notar que, por exemplo, a imagem de $3$ pela composta se obtém da seguinte maneira: $3 \mapsto 4 \mapsto 3$.

Ainda de acordo com essa notação, se

$$f = \begin{pmatrix} \dots & a & \dots & r & \dots & b & \dots \\ \dots & 1 & \dots & i_r & \dots & n & \dots \end{pmatrix}$$

então:

$$f^{-1} = \begin{pmatrix} 1 & \dots & i_r & \dots & n \\ a & \dots & r & \dots & b \end{pmatrix}$$

Por exemplo, em $S_4$ a permutação inversa de

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

é.

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

*Exemplo 4.* Tábuas de $S_2$ e $S_3$.

Obviamente a construção dessas tábuas envolve muitos cálculos. Por brevidade, então, até porque o raciocínio é sempre o mesmo, nos ateremos, em cada caso, a efetuar uma composição apenas. Sugerimos ao leitor verificar os demais resultados.

*Tábua de $S_2$*

Fazendo

$$S_2 = \left\{ f_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

então $f_1 \circ f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = f_0$. Logo:

| $\circ$ | $f_0$ | $f_1$ |
|---|---|---|
| $f_0$ | $f_0$ | $f_1$ |
| $f_1$ | $f_1$ | $f_0$ |

*Tábua de $S_3$*

Façamos

$$S_3 = \left\{ f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Observemos como se obtém $f_1 \circ g_3$, por exemplo:

$$f_1 \circ g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = g_2$$

De maneira análoga se obtêm os demais "produtos". Feito isso e colocando-se esses "produtos" numa tábua, o resultado será o seguinte, como o leitor poderá checar:

| $\circ$ | $f_0$ | $f_1$ | $f_2$ | $g_1$ | $g_2$ | $g_3$ |
|---|---|---|---|---|---|---|
| $f_0$ | $f_0$ | $f_1$ | $f_2$ | $g_1$ | $g_2$ | $g_3$ |
| $f_1$ | $f_1$ | $f_2$ | $f_0$ | $g_3$ | $g_1$ | $g_2$ |
| $f_2$ | $f_2$ | $f_0$ | $f_1$ | $g_2$ | $g_3$ | $g_1$ |
| $g_1$ | $g_1$ | $g_2$ | $g_3$ | $f_0$ | $f_1$ | $f_2$ |
| $g_2$ | $g_2$ | $g_3$ | $g_1$ | $f_2$ | $f_0$ | $f_1$ |
| $g_3$ | $g_3$ | $g_1$ | $g_2$ | $f_1$ | $f_2$ | $f_0$ |

Vale observar também que esse grupo não é abeliano, uma vez que sua tábua não é simétrica em relação à diagonal principal. Por exemplo, $f_2 \circ g_3 = g_1$ ao passo que $g_3 \circ f_2 = g_2$. Como se verá no desenvolvimento da matéria, todo grupo de ordem menor que 6 é comutativo. Outra coisa importante mostrada pela tábua é que o conjunto $C_3 = \{f_0, f_1, f_2\}$ também é um grupo quando considerado com a composição de permutações. De fato, além de ser fechado para a composição, como se vê na tábua, vale a associatividade porque vale em $S_3$, o elemento neu tro $f_0$ está no conjunto, e $f_0^{-1} = f_0$, $f_1^{-1} = f_2$ e $f_2^{-1} = f_1$.

Finalmente, é importante observar ainda na tábua que $f_1^2 = f_1 \circ f_1 = f_2$, $g_1 \circ f_1 = g_2$ e $g_1 \circ f_1^2 = g_1 \circ (f_1 \circ f_1) = g_3$ e que, portanto:

$$S_3 = \{f_1^0, f_1, f_1^2, g_1, g_1 \circ f_1, g_1 \circ f_1^2\}^1$$

Se em vez de $f_2$ tomarmos $f_1$ e em vez de $g_1$ tomarmos $g_2$ ou $g_3$, obteremos uma alternativa equivalente de escrever os elementos do grupo $S_3$. Essa observação é importante porque mostra que é possível escrever ("gerar") todos os elementos do grupo usando-se apenas dois deles.

Mostraremos agora como fica a tábua do grupo $S_3$ com essa forma de escrever seus elementos. Evidentemente é só trocar, na tábua já construída, $f_2$ por $f_1^2$, $g_2$ por $g_1 \circ f_1$ e $g_3$ por $g_1 \circ f_1^2$:

| $\circ$ | $f_1^0$ | $f_1$ | $f_1^2$ | $g_1$ | $g_1 \circ f_1$ | $g_1 \circ f_1^2$ |
|---|---|---|---|---|---|---|
| $f_1^0$ | $f_1^0$ | $f_1$ | $f_1^2$ | $g_1$ | $g_1 \circ f_1$ | $g_1 \circ f_1^2$ |
| $f_1$ | $f_1$ | $f_1^2$ | $f_1^0$ | $g_1 \circ f_1^2$ | $g_1$ | $g_1 \circ f_1$ |
| $f_1^2$ | $f_1^2$ | $f_1^0$ | $f_1$ | $g_1 \circ f_1$ | $g_1 \circ f_1^2$ | $g_1$ |
| $g_1$ | $g_1$ | $g_1 \circ f_1$ | $g_1 \circ f_1^2$ | $f_1^0$ | $f_1$ | $f_1^2$ |
| $g_1 \circ f_1$ | $g_1 \circ f_1$ | $g_1 \circ f_1^2$ | $g_1$ | $f_1^2$ | $f_1^0$ | $f_1$ |
| $g_1 \circ f_1^2$ | $g_1 \circ f_1^2$ | $g_1$ | $g_1 \circ f_1$ | $f_1$ | $f_1^2$ | $f_1^0$ |

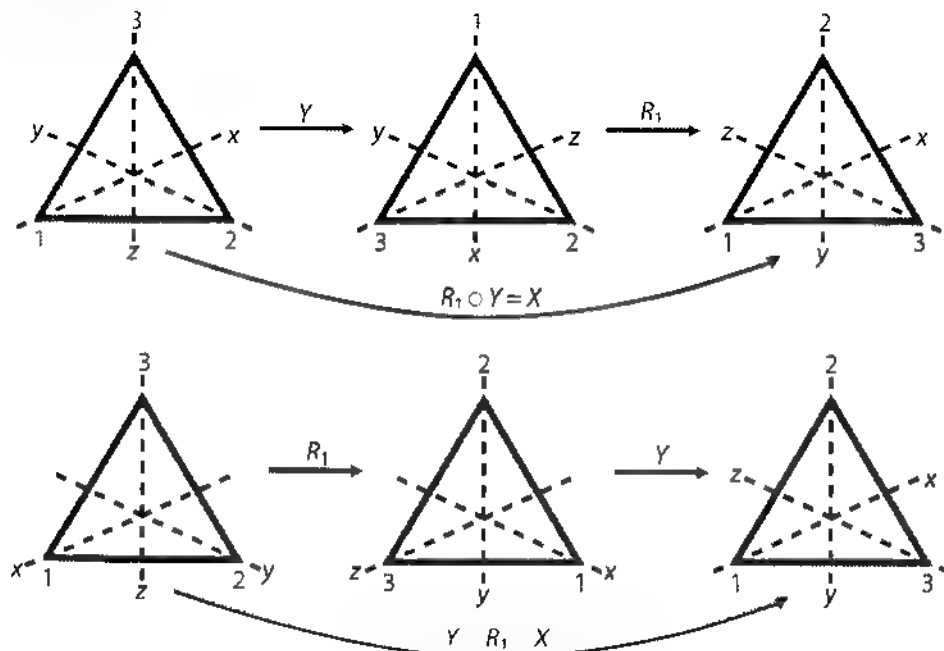
1 Se $a$ é elemento de um grupo cujo elemento neutro é $e$, define-se $a^0 = e$. Portanto, no grupo em estudo, $f_1^0 = f_0$

Notar, por último, que $C_3 \quad \{f_0, f_1, f_2\} = \{f_1{}^0, f_1, f_1{}^2\}$ e, portanto, é possível escrever todos os seus elementos usando-se um deles apenas. Ou seja, $f_1$ gera $C_3$.

(xiii) *Grupos de simetrias*

(xiii-a) *Simetrias do triângulo equilátero*

Denomina-se *simetria* de um triângulo equilátero $T$ qualquer aplicação bijetora[2] $f: T \to T$ que preserva distâncias. *Preservar distâncias* significa que, se $a$ e $b$ são pontos arbitrários do triângulo, então a distância de $f(a)$ a $f(b)$ é igual à distância de $a$ a $b$. Uma isometria pode ser imaginada como uma transformação geométrica que leva uma cópia do triângulo a coincidir com ele próprio.

Para caracterizar geometricamente as simetrias do triângulo, indiquemos seus vértices consecutivamente por 1, 2, 3 e consideremos as seguintes retas pelo baricentro $O$ do triângulo: $x$, pelo vértice 1, $y$, pelo vértice 2, e $z$, pelo vértice 3. Denotando-se por $R_0$, $R_1$ e $R_2$ as rotações de 0, $(2\pi)/3$ e $(4\pi)/3$ radianos em torno de $O$ no sentido anti-horário e por $X$, $Y$ e $Z$, respectivamente, as reflexões espaciais de $\pi$ radianos em torno das retas $x$, $y$ e $z$, prova-se que o conjunto das simetrias do triângulo é exatamente $\{R_0, R_1, R_2, X, Y, Z\}$ (uma demonstração desse fato foge ao alcance deste texto). Mostraremos a seguir, por meio da construção de uma tábua, que esse conjunto, com a composição de transformações, é um grupo não abeliano Para isso, vejamos primeiro (ver figura a seguir) como se obtém geometricamente $R_1 \quad Y$ e $Y \quad R_1$, por exemplo.

2 Na verdade pode-se provar que se f é sobrejetora e preserva distâncias, então f é uma bijeção

Efetuando-se todas as composições possíveis, obtém-se a seguinte tábua:

| ∘ | $R_0$ | $R_1$ | $R_2$ | $X$ | $Y$ | $Z$ |
|---|---|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_1$ | $R_2$ | $X$ | $Y$ | $Z$ |
| $R_1$ | $R_1$ | $R_2$ | $R_0$ | $Z$ | $X$ | $Y$ |
| $R_2$ | $R_2$ | $R_0$ | $R_1$ | $Y$ | $Z$ | $X$ |
| $X$ | $X$ | $Z$ | $Y$ | $R_0$ | $R_2$ | $R_1$ |
| $Y$ | $Y$ | $X$ | $Z$ | $R_1$ | $R_0$ | $R_2$ |
| $Z$ | $Z$ | $Y$ | $X$ | $R_2$ | $R_1$ | $R_0$ |

Por meio dela se verifica o fechamento, que $R_0$ é o elemento neutro e que $R_0^{-1} = R_0, R_1^{-1} = R_2, R_2^{-1} = R_1, X^{-1} = X, Y^{-1} = Y$ e $Z^{-1} = Z$. Valendo a associatividade, por se tratar de composição de transformações, então efetivamente se trata de um grupo. Denotaremos esse grupo por $D_3 = \{R_0, R_1, R_2, X, Y, Z\}$. Como a tábua não é simétrica em relação à diagonal principal, então ele não é abeliano.

Por outro lado, observando-se que $R_1^2 = R_1 \circ R_1 = R_2$, $X \circ R_1 = Z$ e $X \circ R_1^2 = Y$, então:

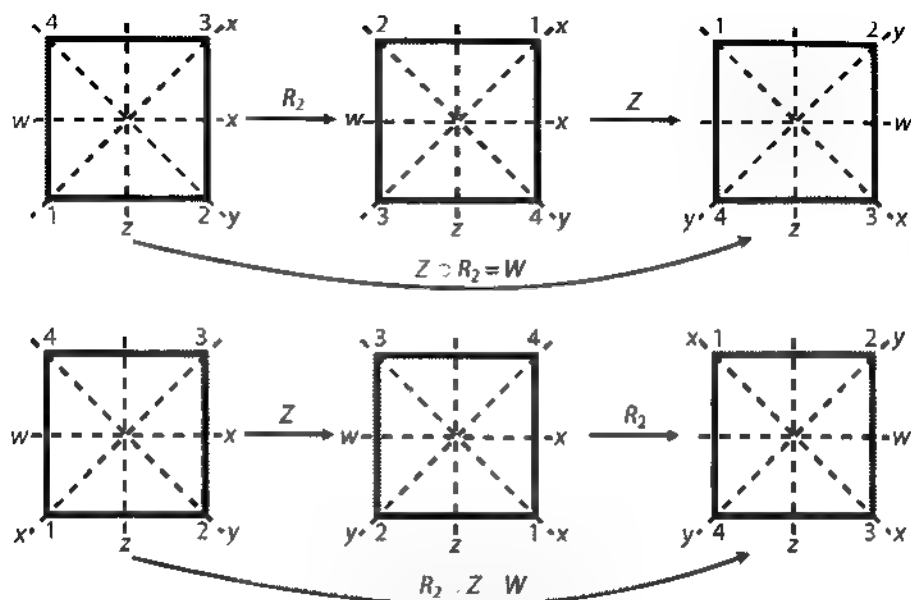
$$D_3 = \{R_1^0, R_1, R_1^2, X, X \circ R_1, X \circ R_1^2\}$$

Ou seja, $D_3$ é gerado por $R_1$ e $X$.

Vale observar ainda que a "partição" mostrada na tábua põe em relevo o seguinte: que a composta de duas rotações é uma rotação; que a composta de duas reflexões é uma rotação; que a composta de uma reflexão com uma rotação ou de uma rotação com uma reflexão é uma reflexão.

(xiii-b) *Simetrias do quadrado*

Uma *simetria* de um quadrado $Q$ é, como se pode induzir do caso do triângulo, uma aplicação bijetora $f: Q \to Q$ que preserva distâncias. E tal como no caso do triângulo, uma isometria pode ser imaginada como uma transformação geométrica que leva uma cópia do quadrado a coincidir com ele próprio.

Para caracterizar geometricamente as simetrias do quadrado, cujo conjunto será indicado por $D_4$, indiquemos seus vértices consecutivamente por 1, 2, 3, 4 e consideremos as retas $x$ e $y$ respectivamente pelas diagonais 13 e 24 do quadrado, e as retas $z$ e $w$ a primeira perpendicular aos lados 12 e 34 pelo ponto médio de ambos e a segunda perpendicular aos lados 23 e 14 também pelo ponto médio de ambos O centro do quadrado, que é interseção dessas retas, será indicado por $O$. Então, denotando-se por $R_0, R_1, R_2, R_3$ as rotações de 0, $\pi/2$, $\pi$ e $3\pi/2$ em torno do ponto $O$, no sentido anti-horário, por $X$ e $Y$ as reflexões de $\pi$ radianos em torno das retas $x$ e $y$ e por $Z$ e $W$ as reflexões de $\pi$ radianos em torno das retas $z$ e $w$, respectivamente, demonstra-se (aqui apenas mencionamos esse fato) que $D_4 = \{R_0, R_1, R_2, R_3, X, Y, Z, W\}$. Por meio da construção de uma tábua, mostraremos agora que esse conjunto, com a composição de transformações, é um grupo A título de ilustração vejamos (figura a seguir) como se obtém, por exemplo, $Z \circ R_2$ e $R_2 \circ Z$

Efetuando-se as demais composições, a tabela obtida é a seguinte (sugerimos ao leitor checar os resultados):

| $\circ$ | $R_0$ | $R_1$ | $R_2$ | $R_3$ | $X$ | $Y$ | $Z$ | $W$ |
|---|---|---|---|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_1$ | $R_2$ | $R_3$ | $X$ | $Y$ | $Z$ | $W$ |
| $R_1$ | $R_1$ | $R_2$ | $R_3$ | $R_0$ | $Z$ | $W$ | $Y$ | $X$ |
| $R_2$ | $R_2$ | $R_3$ | $R_0$ | $R_1$ | $Y$ | $X$ | $W$ | $Z$ |
| $R_3$ | $R_3$ | $R_0$ | $R_1$ | $R_2$ | $W$ | $Z$ | $X$ | $Y$ |
| $X$ | $X$ | $Z$ | $Y$ | $W$ | $R_0$ | $R_2$ | $R_1$ | $R_3$ |
| $Y$ | $Y$ | $W$ | $X$ | $Z$ | $R_2$ | $R_0$ | $R_3$ | $R_1$ |
| $Z$ | $Z$ | $Y$ | $W$ | $X$ | $R_3$ | $R_1$ | $R_0$ | $R_2$ |
| $W$ | $W$ | $X$ | $Z$ | $Y$ | $R_1$ | $R_3$ | $R_2$ | $R_0$ |

Essa tábua mostra imediatamente que a composição de simetrias é uma operação em $D_4$. A associatividade da operação vale por se tratar de particular composição de aplicações. Como, ademais, $R_0$ é o elemento neutro e $R_0^{-1} = R_0$, $R_1^{-1} = R_3$, $R_2^{-1} = R_2$, $R_3^{-1} = R_1$, $X^{-1} = X$, $Y^{-1} = Y$, $Z^{-1} = Z$, $W^{-1} = W$ então $(D_4, \circ)$ é um grupo: o *grupo das simetrias do quadrado*. $D_4$ não é comutativo, pois, por exemplo, $X \circ Z = R_1$ e $Z \circ X = R_3$.

Observando-se que $R_1^2 = R_2$, $R_1^3 = R_1^2 \circ R_1 = R_2 \circ R_1 = R_3$, $X \circ R_1 = Z$, $X \circ R_1^2 = X \circ R_2 = Y$ e $X \circ R_1^3 = X \circ R_3 = W$, então:

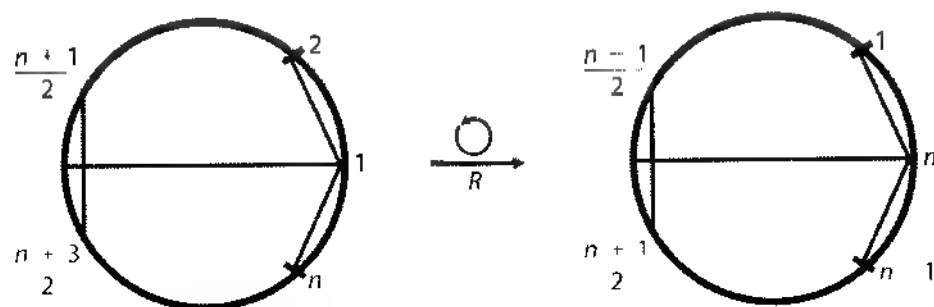
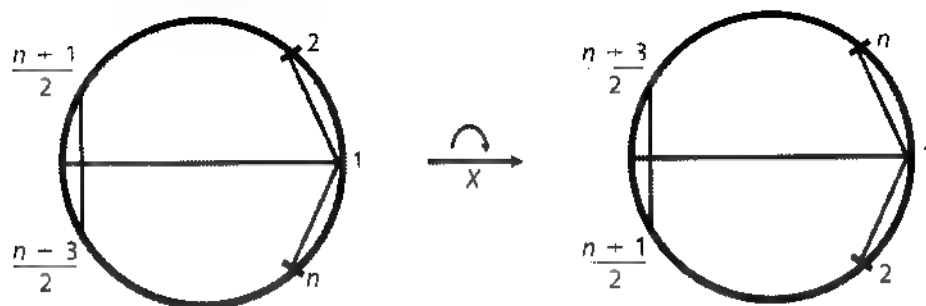
$$D_4 = \{R_1^0, R_1, R_1^2, R_1^3, X, X \circ R_1, X \circ R_1^2, X \circ R_1^3\}$$

isto é, $D_4$ é gerado por $R_1$ e $X$.

Convém notar que a partiçao mostrada na tábua poe em destaque o seguinte: a composta de duas rotações é uma rotação; a composta de duas reflexões é uma rotaçao; e a composta de uma rotação com uma reflexão, ou vice-versa, é uma reflexão. Em particular o conjunto $R_4$ das rotações do quadrado também é um grupo.

(xiv) *Grupos diedrais*

O conceito de simetria de um triângulo e de um quadrado, que acabamos de focalizar, pode ser estendido naturalmente para um polígono regular qualquer de $n$ lados. Tal como nos casos particulares focalizados, o número das simetrias de um polígono regular de $n$ lados é o dobro do número de lados, portanto $2n$ no caso geral.

Para descrever essas simetrias, denotemos os vértices do polígono consecutivamente por 1, 2, ..., $n$ e o conjunto das simetrias por $D_n$. Duas simetrias bastam para gerar $D_n$: a rotação $R$ de $2\pi/n$ radianos em torno do centro $O$ do polígono (figura a seguir)

e a reflexão $X$ de $\pi$ radianos em torno da reta $x$ pelo vértice 1 e pelo centro do polígono (figura a seguir). (Em ambas as figuras consideramos $n$ ímpar.)

Isso posto, pode-se demonstrar que o conjunto das simetrias do polígono é

$$D_n = \{R^0, R, R^2, ..., R^{n-1}, X, X \circ R, X \circ R^2, ..., X \circ R^{n-1}\}$$

e que esse conjunto é um grupo com a composição de transformações. Ou seja, que $D_n$ é um grupo gerado por dois de seus elementos, isto é, a rotação $R$ e a reflexão $X$, resultado que constitui uma generalização do que foi visto para o triângulo e o quadrado

O grupo $D_n$ é chamado *grupo diedral de grau* n. Em particular $D_3$ e $D_4$ são os grupos diedrais de grau 3 e 4, respectivamente.

Outro fato importante envolvendo o grupo diedral $D_n$ é que o conjunto $R_n = \{R^0, R, R^2, \ldots, R^{n-1}\}$ das rotações do polígono é também um grupo em relação à composição de transformações.

(xv) Sejam $G$ e $L$ grupos que, para facilitar, suporemos multiplicativos (para o caso aditivo, por exemplo, bastaria mudar o símbolo da operação). Vejamos como transformar $G \times L$ em um grupo da maneira mais natural possível a partir das operações de $G$ e $L$.

A "multiplicação"

$$((a, b), (c, d)) \mapsto (a, b)(c, d) = (ac, bd)$$

definida para pares quaisquer $(a, b), (c, d) \in G \times L$ certamente é uma operação sobre $G \times L$, a mais natural possível no caso. E com essa operação $G \times L$ ganha uma estrutura de grupo. De fato:

• $[(a, b)(c, d)](e, f) = (ac, bd)(e, f) = ((ac)e, (bd)f) = (a(ce), b(df)) = (a, b)(ce, df) =$ $= (a, b)\ [(c, d)(e, f)]$;

• se $e_G$ e $e_L$ são os elementos neutros de $G$ e $L$, respectivamente, então elemento neutro da "multiplicação de pares" é o par $(e_G, e_L)$;

• se $(a, b) \in G \times L$ e se indicarmos os inversos de $a$ e $b$ em $G$ e $L$ respectivamente por $a'$ e $b'$, então:

$(a, b)(a', b') = (aa', bb') = (e_G, e_L) =$ elemento neutro da "multiplicação" em $G \times L$.

O grupo $G \times L$ assim introduzido será chamado *produto direto* (*externo*) dos grupos $G$ e $L$ dados. Esse novo grupo é comutativo se, e somente se, ambos os grupos fatores o forem.

## 2.5 Subgrupos

Consideremos o grupo $(\mathbb{R}, +)$. Observemos que $\mathbb{Z}$, por exemplo, é um subconjunto de $\mathbb{R}$ para o qual valem as seguintes propriedades: (a) $\mathbb{Z}$ é fechado para a adição; (b) $(\mathbb{Z}, +)$, em que $+$ indica a adição de $\mathbb{R}$, restrita aos elementos de $\mathbb{Z}$, também é um grupo. Por isso se diz que $\mathbb{Z}$ é um *subgrupo* de $\mathbb{R}$. Considerações análogas poderiam ser feitas com $\mathbb{Q}$, por exemplo. Portanto, $\mathbb{Q}$ também é um subgrupo de $\mathbb{R}$

Vejamos agora um exemplo menos corriqueiro. Mantida a notação de **2.4**, consideremos o grupo $S_3 = \{f_0, f_1, f_2, g_1, g_2, g_3\}$ das permutações sobre o conjunto $\{1, 2, 3\}$. A tábua desse grupo nos mostra que o subconjunto $C_3 = \{f_0, f_1, f_2\}$ é fechado para a composição de permutações. Mais: $C_3$, com a composição de permutações, tem uma estrutura de grupo, como já destacamos. Por essa razão, $C_3$ é um *subgrupo* de $S_3$. A definição geral de subgrupo, a ser dada agora, inspira-se em casos como esse.

**Definição 2:** Seja $(G, *)$ um grupo. Diz-se que um subconjunto não vazio $H \subset G$ é um *subgrupo* de $G$ se.

- $H$ é fechado para a operação $*$ (isto é, se $a, b \in H$ então $a * b \in H$);
- $(H, *)$ também é um grupo (aqui o símbolo $*$ indica a restrição da operação de $G$ aos elementos de $H$)

Se $e$ indica o elemento neutro de $G$, então obviamente $\{e\}$ é um subgrupo de $G$ É imediato, também, que o próprio $G$ é um subgrupo de si mesmo. Esses dois subgrupos, ou seja, $\{e\}$ e $G$, são chamados *subgrupos triviais* de $G$.

**Proposição 1:** Seja $(G, *)$ um grupo. Para que uma parte não vazia $H \subset G$ seja um subgrupo de $G$, é necessário e suficiente que $a * b'$ seja um elemento de $H$ sempre que $a$ e $b$ pertencerem a esse conjunto.

*Demonstração:*

$(\rightarrow)$ Indiquemos por $e$ e $e_h$, respectivamente, os elementos neutros de $G$ e $H$. Como

$$e_h * e_h = e_h = e_h * e$$

e todo elemento do grupo é regular em relação a $*$, então $e = e_h$.

Tomemos agora um elemento $b \in H$ e indiquemos por $b'$ e $b_h'$ seus simétricos em $G$ e $H$, respectivamente. Como, porém,

$$b_h' * b = e_h = e = b' * b$$

então $b_h' = b'$ (novamente pelo fato de todos os elementos do grupo serem regulares para sua operação). Por fim, se $a, b \in H$, então $a * b_h' \in H$, uma vez que, por hipótese, $(H, *)$ é um grupo. Mas $b_h' = b'$ e, portanto, $a * b' \in H$.

$(\leftarrow)$ Como, por hipótese, $H$ não é vazio, podemos considerar um elemento $x_0 \in H$. Juntando esse fato à hipótese: $x_0 * x_0' = e \in H$. Considerando agora um elemento $b \in H$, da hipótese e da conclusão anterior segue que:

$$e * b' = b' \in H$$

Mostremos agora que $H$ é fechado para a operação $*$. De fato, se $a, b \in H$, então, levando em conta a conclusão anterior, $a, b' \in H$. De onde (novamente usando a hipótese):

$$a * (b')' = a * b \in H$$

Falta mostrar a associatividade em $H$, mas isso é trivial, pois, se $a, b, c \in H$, então $a, b, c \in G$ e, portanto, $a * (b * c) = (a * b) * c$ (já que essa propriedade vale em $G$). #

Convém *observar* que, se o grupo é aditivo, então a condição de subgrupo dada pela proposição apresenta-se assim:

- Se $a, b \in H$, entao $a + (-b) \in H$.

E no caso de um grupo multiplicativo.

- Se $a, b \in H$, então $ab^{-1} \in H$.

*Exemplo 5:* O conjunto $H = \{x \in \mathbb{R}^* \mid x > 0\}$ é um subgrupo do grupo multiplicativo dos números reais $(\mathbb{R}^*, \cdot)$. De fato, se $a, b \in H$, então $a, b \in \mathbb{R}$, $a > 0$ e $b > 0$. Mas, se $b > 0$, então $b^{-1} > 0$. Logo, $ab^{-1} > 0$, pois o produto de dois números reais estritamente positivos também é estritamente positivo. De onde, $ab^{-1} \in H$.

*Exemplo 6:* Consideremos o grupo aditivo $M_2(\mathbb{R})$. Vamos mostrar, usando a proposição anterior, que

$$H = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R});\ a + d = 0\right\}$$

é um subgrupo de $M_2(\mathbb{R})$. Obviamente trata-se de um conjunto não vazio. Notar primeiro que as matrizes de $H$ se caracterizam pelo fato de os elementos da diagonal principal serem opostos um do outro. Observado isso, tomemos duas matrizes de $H$:

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} r & s \\ t & -r \end{pmatrix}$$

Então:

$$A + (-B) = \begin{pmatrix} a - r & b - s \\ c - t & -a + r \end{pmatrix}$$

Como as entradas dessa matriz obviamente são números reais e $-a + r = -(a - r)$, então $A + (-B) \in H$.

*Exemplo 7:* Consideremos dois grupos, $G$ e $L$, supostos multiplicativos, por simplicidade. Ainda para facilitar, indiquemos os elementos neutros de $G$ e $L$ por 1. Então $\{1\} \times L = \{(x, y) \in G \times L \mid x = 1\}$ e $G \times \{1\} = \{(x, y) \in G \times L \mid y = 1\}$ são subgrupos do produto direto $G \times L$. Faremos a verificação apenas para o segundo caso.

Sejam $\alpha, \beta \in G \times \{1\}$. Então $\alpha = (a, 1)$ e $\beta = (b, 1)$, para convenientes elementos $a, b \in G$. Portanto:

$$\alpha\beta^{-1} = (a, 1)(b, 1)^{-1} = (a, 1)(b^{-1}, 1) = (ab^{-1}, 1)$$

Como $ab^{-1} \in G$, então $\alpha\beta^{-1} \in G \times \{1\}$.

## Exercícios

**1.** Quais dos conjuntos abaixo são grupos em relação à operação indicada?

a) $\mathbb{Z}_-$; adição

b) $\mathbb{Z}_+$; multiplicação

c) $A = \{x \in \mathbb{Z} \mid x \text{ é par}\}$; adição

d) $B = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$; multiplicação

e) $C = \{-2, -1, 0, 1, 2\}$; adição

f) $D = \{1, -1\}$; multiplicação

**2.** Mostre que $\mathbb{R}$ dotado da operação $*$ tal que $x * y = \sqrt[3]{x^3 + y^3}$ é um grupo abeliano

**3.** Mostre que $\mathbb{R}$ munido da operação $\Delta$ tal que $x \,\Delta\, y = x + y - 3$ é um grupo comutativo.

**4.** Mostre que $\mathbb{Q}\left[\sqrt{2}\right] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é um grupo aditivo abeliano. Estabelecer as condições sobre $a$ e $b$ para que $\mathbb{Q}\left[\sqrt{2}\right]$ seja também um grupo multiplicativo.

**5.** Mostre que $\mathbb{R} \times \mathbb{R} - \{(0, 0)\}$ munido da operação $\Delta$ definida por $(a, b) \,\Delta\, (c, d) = (ac - bd, ad + bc)$ é um grupo abeliano.

**6.** No conjunto $\mathbb{C}^*$ está definida uma operação $\Delta$ tal que $a \,\Delta\, b = |a| \cdot b$. Mostre que a operação $\Delta$ não define uma estrutura de grupo sobre $\mathbb{C}^*$.

**7.** Verifique se $\mathbb{Z} \times \mathbb{Z}$ é grupo em relação a cada uma das seguintes leis de composição:

a) $(a, b) * (c, d) = (a + c, b + d)$

b) $(a, b) \Delta (c, d) = (a \cdot c, b \cdot d)$

**8.** Mostre que $\mathbb{Q}^* \times \mathbb{Q}$ munido da operação $\perp$ definida da seguinte forma:

$$(a, b) \perp (c, d) = (ac, bc + d)$$

é um grupo.

**9.** Sejam $(G, *)$ e $(H, \Delta)$ grupos quaisquer. Mostre que $G \times H$ tem estrutura de grupo em relação à operação $\perp$ assim definida: $(x, y) \perp (x', y') = (x * x', y \,\Delta\, y')$, quaisquer que sejam $(x, y)$ e $(x', y')$ em $G \times H$.

**10.** Seja $G$ um grupo multiplicativo e seja $*$ uma operação sobre $G$ assim definida: $a * b = b \cdot a$. Demonstre que $(G, *)$ é um grupo.

**11.** Sejam $A$ um conjunto não vazio e $\mathbb{R}^A$ o conjunto das aplicações de $A$ em $\mathbb{R}$. Definimos uma "adição" e uma "multiplicação" em $\mathbb{R}^A$ como segue. sendo $f$ e $g$ funções de $A$ em $\mathbb{R}$, temos:

$$(f + g)(x) = f(x) + g(x), \forall x \in A$$

$$(f \cdot g)(x) = f(x) \cdot g(x), \forall x \in A$$

Mostre que $\mathbb{R}^A$ é grupo aditivo.

Mostre que, em geral, $\mathbb{R}^A$ não é grupo multiplicativo.

**12.** Mostre que o conjunto das funções polinomiais de grau 1 (ou funções afins) de $\mathbb{R}$ em $\mathbb{R}$ é um grupo para a composição de funções.

*Nota*: $f: \mathbb{R} \to \mathbb{R}$ é uma função afim se, e somente se, $f(x) = ax + b$, com $a \neq 0$.

**13.** Sejam $S$ um conjunto, $G$ um grupo e $f: S \to G$ uma aplicação bijetora Para cada $x, y \in S$ defina o produto $xy = f^{-1}(f(x)f(y))$. Mostre que essa multiplicação define uma estrutura de grupo sobre $S$.

**14.** Construa a tábua da operação $*$ sobre $G = \{e, a\}$, sabendo que $(G, *)$ é um grupo.

**15.** Construa a tábua da operação $*$ sobre $G = \{e, a, b\}$, sabendo que $(G, *)$ é um grupo.

**16.** Mostre que cada uma das tábuas abaixo define uma operação que confere ao conjunto $G = \{e, a, b, c\}$ uma estrutura de grupo.

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $a$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $a$ |

**17.** Complete a tabela abaixo, sabendo que $G = \{e, a, b, c\}$ é um grupo em relação a essa operação.

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | | | |
| $b$ | $b$ | $c$ | | |
| $c$ | $c$ | $e$ | $a$ | |

**18.** Sejam $F_1, F_2, F_3, F_4$ aplicações de $\mathbb{R}^2$ em $\mathbb{R}^2$ definidas da seguinte maneira: $F_1(x, y) = (x, y)$, $F_2(x, y) = (-x, y)$, $F_3(x, y) = (x, -y)$ e $F_4(x, y) = (-x, -y)$. Se $G = \{F_1, F_2, F_3, F_4\}$, mostre que $(G, \circ)$ é um grupo. Obter $F \in G$ tal que $F_2 \circ F \circ F_3 = F_4$.

**19.** Construa a tábua de um grupo $G = \{e, a, b, c, d, f\}$, de ordem 6, sabendo que:

(I) $G$ é abeliano.

(II) O neutro é $e$.

(III) $a*d = b*c = f$

(IV) $a*c = b*b = d$

(V) $a*f = b*d = e$

(VI) $c*d = a$

**20.** Sejam $a, b, c$ elementos de um grupo multiplicativo $G$. Prove que $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$. Obtenha $x \in G$ tal que $abcxb = c$

**21.** Se $a$, $b$ e $c$ são três elementos quaisquer de um grupo multiplicativo $G$, demonstre que existe um único $x \in G$ tal que $axbcx = abx$.

**22.** $G$ é um grupo multiplicativo e $a$ e $b$ são elementos de $G$. Determine $x \in G$ tal que $xax = bba^{-1}$.

**23.** Mostre que, se $x$ é elemento de um grupo multiplicativo e $xx = x$, então $x$ é o elemento neutro.

**24.** Mostre que, se $G$ é um grupo multiplicativo e $xx = 1, \forall x \in G$, então $G$ é abeliano (1 = elemento neutro).

**25.** Seja $G$ um grupo finito. Mostre que, dado $x \in G$, existe um inteiro $n \geqslant 1$ tal que $x^n = e$.

**26.** Sejam $G$ um grupo e $x \in G$. Suponhamos que exista um inteiro $n \geqslant 1$ tal que $x^n = e$. Mostre que existe um inteiro $m \geqslant 1$ tal que $x^{-1} = x^m$.

**27.** Seja $G$ um conjunto finito e munido de uma operação $*$ que é associativa. Mostre que, se a operação $*$ satisfaz as duas leis do cancelamento, então $(G, *)$ é um grupo.

**28.** Verifique se $A$ ou $B$ é subgrupo do grupo multiplicativo $\mathbb{Q}^*$.

$A = \{x \in \mathbb{Q} \mid x > 0\}$

$B = \left\{\frac{1 + 2m}{1 + 2n} \mid m, n \in \mathbb{Z}\right\}$

**29.** Verifique se $A$ ou $B$ é subgrupo do grupo multiplicativo $\mathbb{R}^*$.

$A = \{a + b\sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$

$B = \{a + b\sqrt[3]{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$

**30.** Verifique se $A$ ou $B$ é subgrupo do grupo multiplicativo $\mathbb{C}^*$.

$A = \{\cos\theta + i \cdot \operatorname{sen}\theta \mid \theta \in \mathbb{R}\}$

$B = \{z \in \mathbb{C} \mid |z| = 2\}$

**31.** Verifique se $A$ ou $B$ é subgrupo do grupo aditivo $\mathbb{R}$, supondo $p \in \mathbb{N}$ um número primo dado:

$A = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$

$B = \{a + b\sqrt[3]{p} \mid a, b \in \mathbb{Q}\}$

**32.** Sabendo que $\mathbb{Q} - \{1\}$ é um grupo relativamente à operação $*$ tal que $x * y = x + y - xy$, verifique se $A = \{0, \pm 2, \pm 4, \dots\}$ é ou não um subgrupo desse grupo.

**33.** Mostre o conjunto G das matrizes do tipo $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, com $a, b \in \mathbb{R}$ e $a$ e $b$ não nulos simultaneamente, constitui um subgrupo do grupo $GL_2(\mathbb{R})$
($GL_2(\mathbb{R})$ indica o grupo multiplicativo das matrizes reais inversíveis $2 \times 2$.)

**34.** Mostre que o conjunto $H$ das matrizes do tipo $\begin{pmatrix} \cos a & \operatorname{sen} a \\ -\operatorname{sen} a & \cos a \end{pmatrix}$, com $a \in \mathbb{R}$, constitui um subgrupo do grupo multiplicativo $GL_2(\mathbb{R})$ das matrizes reais e inversíveis do tipo $2 \times 2$.

**35.** Para todo $n \in \mathbb{N}^*$, o conjunto $\mathbb{R}^n$ é definido da seguinte forma:

$$\mathbb{R}^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{R}\}$$

Sabendo que $\mathbb{R}^n$ é um grupo em relação à adição assim definida:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

verifique se $H_1$, $H_2$ e $H_3$ são subgrupos de $\mathbb{R}^n$.

$H_1 = \{(a_1, a_2, \dots, a_n) \in \mathbb{R}^n \mid a_1 + a_2 + \dots + a_n = 0\}$
$H_2 = \{(a_1, a_2, \dots, a_n) \in \mathbb{R}^n \mid a_1 \in \mathbb{Z}\}$
$H_3 = \{(a_1, a_2, \dots, a_n) \in \mathbb{R}^n \mid a_1 \geqslant a_2 \geqslant \dots \geqslant a_n\}$

**36.** Quais dos seguintes subconjuntos de $\mathbb{Z}_{13}$ são grupos em relação à multiplicação?

a) $\{\overline{1}, \overline{12}\}$
b) $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}\}$
c) $\{\overline{1}, \overline{5}, \overline{8}, \overline{12}\}$

**37.** Determine todos os subgrupos do grupo aditivo $\mathbb{Z}_4$.

**38.** Seja $E = \{e, a, b, c, d, f\}$ munido da operação $\Delta$ dada pela seguinte tábua:

| $\Delta$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $b$ | $e$ | $f$ | $c$ | $d$ |
| $b$ | $b$ | $e$ | $a$ | $d$ | $f$ | $c$ |
| $c$ | $c$ | $d$ | $f$ | $e$ | $a$ | $b$ |
| $d$ | $d$ | $f$ | $c$ | $b$ | $e$ | $a$ |
| $f$ | $f$ | $c$ | $d$ | $a$ | $b$ | $e$ |

a) Admitindo a propriedade associativa, prove que $(E, \Delta)$ é um grupo não comutativo.

b) Obtenha os subgrupos de $E$ com ordem 2 ou 3.

**39.** Seja $E = \{e, a, b, c, d, f\}$ munido da operação $\odot$ dada pela seguinte tábua

| $\odot$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $f$ | $e$ |
| $b$ | $b$ | $e$ | $d$ | $f$ | $e$ | $a$ |
| $c$ | $c$ | $d$ | $f$ | $e$ | $a$ | $b$ |
| $d$ | $d$ | $f$ | $e$ | $a$ | $b$ | $c$ |
| $f$ | $f$ | $e$ | $a$ | $b$ | $c$ | $d$ |

a) Admitindo a propriedade associativa, prove que $(E, \odot)$ é um grupo comutativo.

b) Obtenha os subgrupos de $E$ com ordem 2 ou 3.

**40.** Mostre que $H \subset \mathbb{Z}$ é um subgrupo do grupo aditivo $\mathbb{Z}$ se, e somente se, existe um $m \in H$ de modo que $H = \{km \mid k \in \mathbb{Z}\}$.

*Nota:* Se $m \in \mathbb{Z}$, então o subgrupo $\{km \mid k \in \mathbb{Z}\}$ costuma ser denotado por $m\mathbb{Z}$.

**41.** Prove que, se $H_1$ e $H_2$ são subgrupos do grupo $G$, então $H_1 \cap H_2$ também é subgrupo de $G$.

**42.** Prove que, se $H_1$ e $H_2$ são subgrupos de um grupo $G$, então $H_1 \cup H_2$ é subgrupo de $G$ se, e somente se, $H_1 \subset H_2$ ou $H_2 \subset H_1$.

**43.** Seja $G$ um grupo multiplicativo e seja $a$ um elemento de $G$. Prove que $N(a) = \{x \in G \mid ax = xa\}$ é um subgrupo de $G$.

**44.** Construa a tábua do grupo $G = \{0, 1, 2, 3, 4, 5\}$ com a operação $\oplus$ assim definida:

$$x \oplus y = \text{resto da divisão em } \mathbb{Z} \text{ de } x + y \text{ por } 6$$

Quais são os subgrupos de $G$?

**45.** Seja $S$ um subgrupo de um grupo $G$ e defina $T = \{x \in G \mid Sx = xS\}$ Mostre que $T$ é um subgrupo de $G$. ($Sx = \{sx \mid s \in S\}$; $xS = \{xs \mid s \in S\}$.)

**46.** Seja $G$ um grupo multiplicativo e seja $H$ uma parte não vazia e finita de $G$ tal que $HH \subset H$; demonstre que $H$ é subgrupo de $G$. ($H \cdot H = \{h_1 h_2 \mid h_1, h_2 \in H\}$).

**47.** Sejam $A$ e $B$ dois subgrupos de um grupo $G$. Demonstre que $AB = \{ab \mid a \in A$ e $b \in B\}$ é um subgrupo de $G$ se, e somente se, $AB = BA$.

## Exercícios complementares

**C1.** Mostre que, se $G$ é um grupo multiplicativo finito com número par de elementos, então existe um elemento $x \neq 1$ ($1$ = elemento neutro) em $G$ tal que $x = x^{-1}$.
*Sugestão:* Faça $G = A \cup B$ em que $A = \{x \in G \mid x \neq x^{-1}\}$ e $B = \{x \in G \mid x = x^{-1}\}$

**C2.** Sejam $G$ um grupo e $H$ um subgrupo. Seja $x \in G$. Seja ainda $xHx^{-1}$ o subconjunto de $G$ formado por todos os elementos $xyx^{-1}$ com $y \in H$. Mostre que $xHx^{-1}$ é um subgrupo de $G$.

**C3.** Sejam $G$ um grupo e $a$ um elemento de $G$. Seja $\sigma_a: G \to G$ a aplicação tal que $\sigma_a(x) = axa^{-1}$. Mostre que o conjunto de todas as aplicações $\sigma_a$, com $a \in G$, é um grupo com a composição de aplicações.

# IV-2 HOMOMORFISMOS E ISOMORFISMOS DE GRUPOS

## 3. INTRODUÇÃO

O objetivo principal deste tópico é introduzir o conceito de "isomorfismo" de grupos e estudar suas propriedades básicas. A idéia por trás desse conceito é a de separar os grupos em classes disjuntas tais que as propriedades deduzidas para um particular grupo de uma dada classe possam ser transferidas para todos os grupos dessa classe, e apenas para estes, com uma mudança adequada das notações. Essencialmente, dois grupos de uma mesma classe são indistinguíveis em tudo que é pertinente à teoria dos grupos (e apenas quanto a isso). E para que dois grupos, $G$ e $H$, pertençam à mesma classe, exige-se que se possa definir uma bijeção $f: G \to H$ que "preserve as operações". A bijeção garante a necessidade óbvia de que $G$ e $H$ tenham a mesma cardinalidade, ao passo que "preservar as operações" significa, grosso modo, a possibilidade de poder transferir os "cálculos" de um para o outro. No próximo item, formalizaremos essa idéia.

Embora essa formalização esteja associada ao desenvolvimento da álgebra moderna e, portanto, seja relativamente recente na história da matemática, sua utilização informal e despercebida em outras áreas é muito antiga. Como exemplo, consideremos a congruência de triângulos, já estudada por Euclides em seus *Elementos* (c. 300 a.C.). O objetivo da congruência é separar os triângulos em classes disjuntas segundo o critério métrico. Assim, ao se achar, por exemplo, a área de um dado triângulo na verdade está se achando a área de todos os triângulos que lhe são congruentes, ou seja, de todos os triângulos da mesma classe.

Um exemplo mais específico do uso informal e despercebido dessa idéia ocorreu no começo do século XVII, com a criação dos logaritmos. Estes foram introduzidos na matemática com uma finalidade que perdeu totalmente o sentido mais ou menos a partir dos anos 1960, com o advento dos computadores e calculadoras: socorrer os matemáticos, e especialmente os astrônomos, em seus longos e penosos cálculos aritméticos. A idéia era transformar uma multiplicação, uma divisão ou uma radiciação respectivamente numa adição, subtração ou divisão por um número inteiro, certamente operações bem mais fáceis de efetuar de modo geral. Notavelmente os logaritmos criados por John Napier (1550-1617) com essa finalidade cumpriam plenamente o papel esperado. Para isso Napier construiu uma tábua de logaritmos, publicada em 1614. Assim, para calcular, por exemplo, o produto de dois números estritamente positivos, achavam-se, por meio da tábua, seus "logaritmos" no campo dos números reais; a seguir somavam-se esses logaritmos; finalmente, ainda por meio da tábua, mas voltando atrás, procurava-se o número positivo cujo logaritmo fosse a soma encontrada. Esse número era o produto desejado. Evidentemente sem perceber, Napier estava procedendo a uma forma de identificação do grupo $(\mathbb{R}^*_+, \cdot)$ (ver exemplo 5) com o grupo $(\mathbb{R}, +)$. O procedimento de Napier era diferente, mas hoje essa identificação formalmente se faz por meio de uma aplicação bijetora

$$\log\colon \mathbb{R}^*_+ \to \mathbb{R}$$

que transforma produtos em somas mediante a propriedade

$$\log(ab) = \log(a) + \log(b).$$

## 4. HOMOMORFISMOS DE GRUPOS

**Definição 3:** Dá-se o nome de *homomorfismo* de um grupo $(G, *)$ num grupo $(J, .)$ a toda aplicação $f\colon G \to J$ tal que, quaisquer que sejam $x, y \in G$:

$$f(x * y) = f(x) \cdot f(y)$$

Nessas condições, para simplificar a linguagem, nos referiremos a $f\colon G \to J$ como um *homomorfismo de grupos*. Quando se tratar do mesmo grupo, o que pressupõe $J = G$ e a mesma operação, então $f$ será chamada de *homomorfismo* de $G$.

Se um homomorfismo é uma aplicação injetora, então é chamado de *homomorfismo injetor*. E se for uma aplicação sobrejetora, de *homomorfismo sobrejetor*. O caso em que $f$ é bijetora corresponde ao conceito de *isomorfismo* e será estudado separadamente.

G
J
$x$
$y$
$x * y$
$f(x)$
$f(y)$
$f(x) \cdot f(y)$

*Exemplo 8:* A aplicação $f: \mathbb{Z} \to \mathbb{C}^*$ definida por $f(m) = i^m$ é um homomorfismo de grupos. É preciso notar, primeiro, que em casos como esses as operações são as usuais e devem ser pressupostas. Portanto, $\mathbb{Z}$ é um grupo aditivo e $\mathbb{C}^*$ um grupo multiplicativo. Como

$$f(m + n) = i^{m+n} = i^m \cdot i^n = f(m) \cdot f(n)$$

fica provado que se trata de homomorfismo.

Esse homomorfismo não é injetor. Para mostrar isso basta um contra-exemplo. De fato $f(4) = i^4 = 1$ e $f(0) = i^0 = 1$. Também não é sobrejetor, pois $\text{Im}(f) = \{1, i, -1, -i\} \neq \mathbb{C}^*$.

*Exemplo 9:* A aplicação $f: \mathbb{C}^* \to \mathbb{R}^*_+$ definida por $f(z) = |z|$ é um homomorfismo sobrejetor. Lembrar primeiro que se trata de dois grupos multiplicativos. Então, como

$$f(zw) = |zw| = |z||w| = f(z)f(w)$$

fica provado que $f$ é homomorfismo. Por outro lado, se $a$ é um número real estritamente positivo, então o próprio $a$ tem imagem igual a $a$ pela aplicação $f$, pois $f(a) = |a| = a$ e, portanto, $f$ é sobrejetora. Na verdade, todos os números complexos que têm afixos na circunferência de centro na origem e raio $a$ têm módulo $a$ e, portanto, imagem $a$ pela aplicação $f$. O fato de os infinitos números complexos com afixos na circunferência terem a mesma imagem basta para mostrar que $f$ não é um homomorfismo injetor.

*Exemplo 10:* Seja $a$ um número inteiro dado. A aplicação $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(m) = am$ é um homomorfismo de $\mathbb{Z}$. Esse homomorfismo só não é injetor quando $a = 0$ e só é sobrejetor quando $a = 1$.

Quanto à primeira afirmação, basta observar que

$$f(m + n) = a(m + n) = am + an = f(m) + f(n)$$

Se $a = 0$, então $f(m) = 0$, para todo $m \in \mathbb{Z}$, e, portanto, $f$ não é injetora nem sobrejetora. Suponhamos $a \neq 0$ e $f(m) = f(n)$, isto é, $am = an$; cancelando-se $a$ (o que é possível, pois $a \neq 0$), obtém-se $m = n$; isso mostra que $f$ é injetora neste caso.

Se $a = 1$, então $f$ é a aplicação idêntica de $\mathbb{Z}$ e, portanto, é sobrejetora. Se $a \neq 1$, então $f$ não é sobrejetora, porque $\text{Im}(f) = \{0, \pm a, \pm 2a, \pm 3a, \ldots\} \neq \mathbb{Z}$.

*Exemplo 11.* Dado um inteiro $m > 1$, consideremos $p_m: \mathbb{Z} \to \mathbb{Z}_m$ definida por $p_m(a) = \bar{a}$. Então $p_m$ é um homomorfismo sobrejetor de grupos, pois: (i) $p_m(a + b) = \overline{a + b} = \bar{a} + \bar{b} = p_m(a) + p_m(b)$; (ii) se $y \in \mathbb{Z}_m$, então $y = \bar{a}$, para algum $a \in \{0, 1, 2, \ldots, m - 1\}$, e, portanto, $p_m(a) = \bar{a} = y$.

## 5. PROPOSIÇÕES SOBRE HOMOMORFISMOS DE GRUPOS

Nas proposições a serem focalizadas neste item, usaremos, por simplicidade, a notação multiplicativa para indicar as operações dos grupos considerados. Como observamos em **2.2**, isso não acarreta nenhuma perda de generalidade e a passagem dos resultados obtidos mediante essa notação para qualquer outro caso é simplesmente uma questão de mudança de símbolos.

Isso posto, sejam $G$ e $J$ grupos multiplicativos cujos elementos neutros indicaremos sempre por $e$ e $u$, respectivamente, e $f: G \to J$ um homomorfismo de grupos.

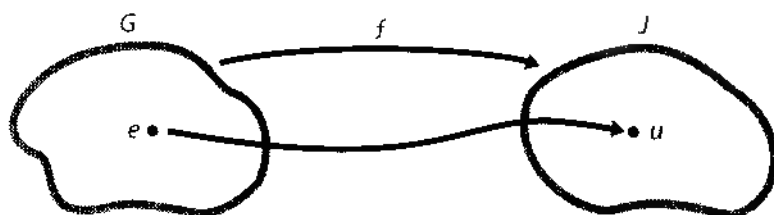
**Proposição 2:** $f(e) = u$.

*Demonstração:* Obviamente $ee = e$ (pois $e$ é o elemento neutro de $G$) e $uf(e) = f(e)$ (pois $f(e) \in J$ e $u$ é o elemento neutro de $J$). Levando-se em conta isso e a hipótese de que $f$ é um homomorfismo:

$$\underline{f(e)f(e)} = f(ee) = f(e) = \underline{uf(e)}$$

$$\downarrow$$

$$f(e) = u$$

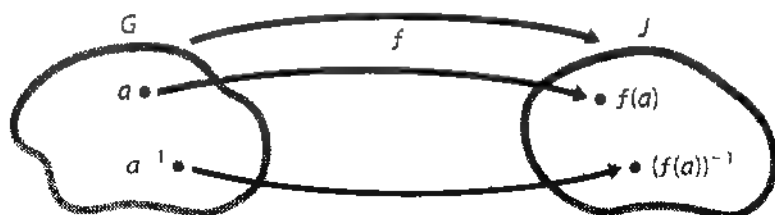
(pois todo elemento de um grupo é regular). #

**Proposição 3:** Se $a$ é um elemento qualquer de $G$, então $f(a^{-1}) = [f(a)]^{-1}$.

*Demonstração:* Usaremos aqui a proposição anterior:

$$\underline{f(a)f(a^{-1})} = f(aa^{-1}) = f(e) = u = \underline{f(a)[f(a)]^{-1}}$$

$$\downarrow$$

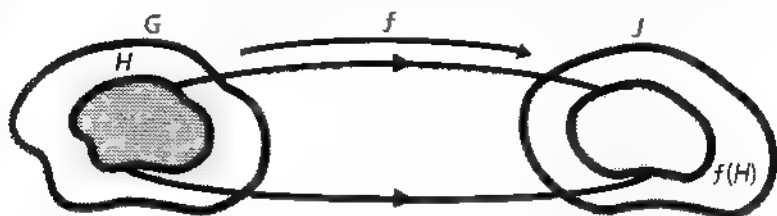
$$f(a^{-1}) = [f(a)]^{-1}$$

(mesmo motivo da demonstração anterior). #

**Corolário:** $f(ab^{-1}) = f(a)[f(b)]^{-1}$.

**Proposição 4:** Se $H$ é um subgrupo de $G$, então $f(H)$ é um subgrupo de $J$

*Demonstração:* Lembremos primeiro que $f(H) = \{f(x) \mid x \in H\}$.

(i) Como $e \in H$, porque $H$ é um subgrupo de $G$, então $f(e) = u \in f(H)$ e, portanto, $f(H) \neq \emptyset$.

(ii) Sejam $c, d \in f(H)$. Então $c = f(a)$ e $d = f(b)$, para convenientes elementos $a, b \in H$. Logo, $cd^{-1} = f(a)[f(b)]^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Como $ab^{-1} \in H$, pois, por hipótese, $H$ é um subgrupo de $G$, então $cd^{-1} \in f(H)$. #

Em outros termos, a proposição anterior garante que um homomorfismo de grupos $f: G \to J$ transforma subgrupos de $G$ em subgrupos de $J$. Em particular, $\text{Im}(f)$ é um subrupo de $J$.

**Proposição 5:** Sejam $G$, $J$ e $L$ grupos. Se $f: G \to J$ e $g: J \to L$ são homomorfismos de grupos, então o mesmo se pode dizer de $g \circ f: G \to L$.

*Demonstração:* Se $a, b \in G$, então:

$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)\,(g \circ f)(b)$. #

**Corolário:** Se $f$ e $g$ são homomorfismos injetores (sobrejetores), então $g \circ f$ também é um homomorfismo injetor (sobrejetor).

*Demonstração:* Imediata. É só lembrar que a composta de duas funções injetoras (sobrejetoras) também é injetora (sobrejetora).

## 6. NÚCLEO DE UM HOMOMORFISMO

**Definição 4:** Seja $f: G \to J$ um homomorfismo de grupos. Se $u$ indica o elemento neutro de $J$, o seguinte subconjunto de $G$ será chamado *núcleo de f* e denotado por $N(f)$ (na literatura é comum também a notação $Ker(f)$)[3]:

$$N(f) = \{x \in G \mid f(x) = u\}$$

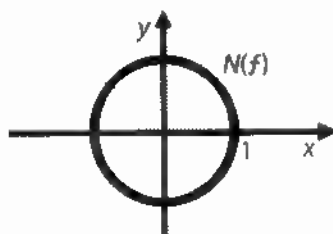
Vale observar que, como $f(e) = u$ (proposição 2), então $e \in N(f)$. Assim, pelo menos o elemento neutro de $G$ pertence ao núcleo de $f$.

*Exemplo 12:* Procuremos o núcleo do homomorfismo de grupos $f: \mathbb{Z} \to \mathbb{C}^*$ definido por $f(m) = i^m$ (ver exemplo 8). Como o elemento neutro de $\mathbb{C}^*$ é o numero 1, en-

3 De *kernel* do inglês, que significa "caroço" ou "semente" e, em sentido figurado, "cerne".

tao basta resolver a equação $i^m = 1$. Mas, como é bem conhecido do estudo dos números complexos, o conjunto das soluções dessa equação, ou seja, o nucleo de $f$, é:

$$N(f) = \{0, \pm 4, \pm 8, ...\}$$

*Exemplo 13:* Consideremos o homomorfismo $f: \mathbb{C}^* \to \mathbb{R}^*_+$ definido por $f(z) = |z|$ (ver exemplo 9). Como o elemento neutro de $\mathbb{R}^*_+$ é o número 1, então temos de encontrar as soluções de $|z| = 1$; ou seja, o núcleo é formado por todos os números complexos de módulo igual a 1. Como também é sabido, são infinitos esses números complexos: todos aqueles cujos afixos se situam na circunferência de centro na origem e raio 1.

*Exemplo 14:* Consideremos agora o homomorfismo $f: \mathbb{Z} \to \mathbb{Z}$ definido por $f(m) = am$, em que $a$ é um número inteiro dado (ver exemplo 10). Como o elemento neutro de $\mathbb{Z}$ é o número 0, temos de resolver a equação $am = 0$. Mas é claro que o conjunto das soluções depende de $a$. Se $a = 0$, então o núcleo é $\mathbb{Z}$, pois, para todo inteiro $m$, vale a igualdade $m \cdot 0 = 0$. Mas, se $a \neq 0$, então a única solução de $am = 0$ é o número 0, e, portanto, neste caso, $N(f) = \{0\}$.

**Proposição 6:** Seja $f: G \to J$ um homomorfismo de grupos. Então. (i) $N(f)$ é um subgrupo de $G$; (ii) $f$ é um homomorfismo injetor se, e somente se, $N(f) = \{e\}$.

*Demonstração:*

(i) Como $f(e) = u$ (proposição 2), então $e \in N(f)$ e, portanto, $N(f) \neq \emptyset$. Por outro lado, se $a, b \in N(f)$, então $f(a) = f(b) = u$ e, portanto:

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = uu^{-1} = u$$

Isso mostra que $ab^{-1} \in N(f)$.

(ii) ($\to$) Por hipótese, $f$ é injetor e temos de mostrar que o único elemento de $N(f)$ é $e$ (elemento neutro de G). Para isso, vamos tomar $a \in N(f)$ e demonstrar que necessariamente $a = e$. De fato, como $a \in N(f)$, então $f(a) = u$. Mas, devido à proposição 2, $f(e) = u$. Portanto, $f(a) = f(e)$. Como, porém, $f$ é injetora, por hipótese, então $a = e$.

($\leftarrow$) Sejam $x_1, x_2 \in G$ elementos tais que $f(x_1) = f(x_2)$. Multiplicando-se cada membro dessa igualdade por $[f(x_2)]^{-1}$, obtém-se $f(x_1)[f(x_2)]^{-1} = u$. Mas, devido ao corolário da proposição 3, $f(x_1)[f(x_2)]^{-1} = f(x_1x_2^{-1})$. Portanto, $f(x_1x_2^{-1}) = u$, o que mostra que $x_1x_2^{-1} \in N(f) = \{e\}$. Então $x_1x_2^{-1} = e$ e, portanto, $x_1 = x_2$. De onde, $f$ é injetor, como queríamos provar. #

*Exemplo 15.* Dos homomorfismos focalizados nos exemplos 12, 13 e 14, só é njetor o último, quando $a \neq 0$.

## 7. ISOMORFISMOS DE GRUPOS

A idéia de isomorfismo já foi esboçada no início desta seção. Mas, dada a sua importância, convém mais uma vez chamar a atenção para seus elementos básicos através de um exemplo simples.

Consideremos o grupo multiplicativo $G = \{1, -1\}$ e o grupo $S_2$ das permutações sobre o conjunto $\{1, 2\}$. Lembrar que

$$S_2 = \left\{f_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}; f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\right\}$$

e a operação, neste caso, é a composição de permutações.

Observando as tábuas desses grupos:

$G$

| $\cdot$ | $1$ | $-1$ |
|---|---|---|
| $1$ | $1$ | $-1$ |
| $-1$ | $1$ | $1$ |

$S_2$

| $\circ$ | $f_0$ | $f_1$ |
|---|---|---|
| $f_0$ | $f_0$ | $f_1$ |
| $f_1$ | $f_1$ | $f_0$ |

verificamos que, salvo quanto ao "nome" dos elementos e das operações, elas são idênticas. Mais precisamente, se na segunda tábua substituirmos $\circ$ por $\cdot$, $f_0$ por 1 e $f_1$ por $-1$, obteremos a tábua de $G$.

Formalmente, isso poderia ser traduzido pelo fato de que a aplicação $\sigma: G \to S_2$, definida por $\sigma(1) = f_0$ e $\sigma(-1) = f_1$, que obviamente é bijetora, "preserva" as operações, no sentido de que:

$$1 \cdot 1 = 1 \;\mapsto\; f_0 = f_0 \circ f_0 = \sigma(1)\sigma(1)$$
$$1 \cdot (-1) = -1 \;\mapsto\; f_1 = f_0 \circ f_1 = \sigma(1)\sigma(-1)$$
$$(-1) \cdot (-1) = 1 \;\mapsto\; f_0 = f_1 \circ f_1 = \sigma(-1)\sigma(-1)$$

Visto que a aplicação bijetora $\sigma$, apesar de trocar os nomes dos elementos envolvidos, "preserva" as operações, os grupos podem ser considerados indistintos na medida em que forem vistos apenas como grupos. Daí ser possível até substituir um pelo outro se isso for conveniente.

A definição que segue deriva de situações como essa.

**Definição 5:** Seja $f: G \to J$ um homomorfismo de grupos. Se $f$ for também uma bijeção, então será chamado de *isomorfismo do grupo G no grupo J*. Neste caso, diz-se que $f$ é um *isomorfismo de grupos*. Se $G = J$ e a operação é a mesma, $f$ é um *isomorfismo de G*.

*Exemplo 16:* A função logarítmica (não importa a base) log: $\mathbb{R}_+^* \to \mathbb{R}$ é um isomorfismo de grupos porque, devido a pré-requisitos para este trabalho:

- $\log(xy) = \log(x) + \log(y)$, isto é, log preserva as operações envolvidas (a multiplicação de $\mathbb{R}_+^*$ e a adição de $\mathbb{R}$);
- log é uma bijeção.

*Exemplo 17:* Consideremos o produto direto $G \times L$ dos grupos $G$ e $L$. Como já vimos (exemplo 7), $\{1\} \times L$ e $G \times \{1\}$ são subgrupos desse grupo. Portanto, ambos são grupos para a operação de $G \times L$ restrita a seus elementos. Isso posto, pode-se mostrar que o primeiro deles é isomorfo a $L$ e o segundo a $G$. A demonstração é análoga nos dois casos e, portanto, vamos nos limitar a fazê-la para o primeiro. Numa questão como esta é preciso, inclusive, descobrir o isomorfismo. Mas isso não é difícil, observando-se como são os elementos genéricos de um e outro grupos. Se um elemento genérico de $L$ é $a$, então um elemento genérico de $\{1\} \times L$ é $(1, a)$. Assim, é razoável experimentar a aplicação $f: L \to \{1\} \times L$ definida por $f(a) = (1, a)$. Vejamos.

- Se $f(a) = f(b)$ então $(1, a) = (1, b)$ e, portanto, $a = b$. De onde, $f$ é injetora.
- Se $y \in \{1\} \times L$ então $y = (1, x)$, para algum $x \in L$. Como $f(x) = (1, x) = y$, fica provado que $f$ também é sobrejetora.
- $f(ab) = (1, ab) = (1, a)(1, b) = f(a)f(b)$ e, portanto, $f$ é um homomorfismo de grupos.

**Proposição 7:** Se $f: G \to J$ é um isomorfismo de grupos, então $f^{-1}: J \to G$ também é um isomorfismo de grupos.

*Demonstração:* Lembremos primeiro que, como foi provado no capítulo III, o fato de $f$ ser uma bijeção garante que $f^{-1}$ também é uma aplicação bijetora, só que obviamente de $J$ em $G$.

Assim, falta demonstrar que $f^{-1}$ conserva as operações (mais uma vez aqui indicadas multiplicativamente). Para isso, tomemos $y_1, y_2 \in J$. Como $f$ é sobrejetora, $y_1 = f(x_1)$ e $y_2 = f(x_2)$, para convenientes elementos $x_1, x_2 \in G$. Daí, $f^{-1}(y_1) = f^{-1}(f(x_1)) = x_1$ e, analogamente, $f^{-1}(y_2) = x_2$. Então:

$$f^{-1}(y_1y_2) = f^{-1}(f(x_1)f(x_2)) = f^{-1}(f(x_1x_2)) = x_1x_2 = f^{-1}(y_1)f^{-1}(y_2). \#$$

Em face do resultado anterior, se $f: G \to J$ é um isomorfismo de grupos, então pode-se dizer que os grupos $G$ e $J$ são *isomorfos*. Por exemplo, os grupos $(\mathbb{R}_+^*, \cdot)$ e $(\mathbb{R}, +)$ são isomorfos, via uma função logarítmica.

## 8. O TEOREMA DE CAYLEY

Como já vimos, a natureza dos grupos varia amplamente: por exemplo, há grupos de números, grupos de permutações e grupos de matrizes, entre outros. O objetivo central desta seção é dar uma demonstração de que, a despeito disso, há um certo elo entre todos eles. Ocorre que, como mostraremos, todo grupo é isomorfo a um conveniente grupo de permutações. O teorema de Cayley, que garante esse fato, é um exemplo do que se chama em matemática de *teorema de representação*. O fato de todo grupo poder ser representado por um grupo de permutações tem a vantagem de dar um certo caráter de concretude ao grupo em estudo, por mais abstrato que este seja.

**Definição 6:** Seja $G$ um grupo (continuaremos, para facilitar, com a notação multiplicativa). Para cada $a \in G$, a aplicação

$$\delta_a: G \to G$$

tal que $\delta_a(x) = ax$, para qualquer $x \in G$, será chamada *translação à esquerda definida por a*. De maneira análoga se definiria *translação à direita*.

No caso de $G$ ser um grupo aditivo, a translação à esquerda definida por um elemento $a \in G$ é assim definida: $\delta_a(x) = a + x$.

Nas considerações a seguir, é indiferente usar translações à esquerda ou à direita, mas usaremos as primeiras.

**Proposição 8:** Toda translação é uma bijeção, ou seja, é uma permutação dos elementos de $G$.

*Demonstração:* Seja $\delta_a$ uma translação de $G$ e suponhamos $\delta_a(x) = \delta_a(y)$. Então $ax = ay$ e, portanto, $x = y$, uma vez que todo elemento de um grupo é regular. Isso mostra que $\delta_a$ é injetora. Para mostrar que é sobrejetora, dado um elemento qualquer $y \in G$, deve ser possível encontrar $x \in G$ tal que $ax = y$. Mas, como já vimos, essa equação tem solução no grupo: o elemento $a^{-1}y \in G$. Então $\delta_a$ é sobrejetora.

Adotando-se a notação $T(G)$ para indicar o conjunto das translações em $G$ e lembrando que $S(G)$ foi a notação adotada para o conjunto das permutações dos elementos de $G$, então a proposição anterior nos diz que $T(G) \subset S(G)$. #

**Proposição 9:** (i) A composição de translações é uma operação sobre $T(G)$; (ii) a inversa da translação $\delta_a$ é a translação $\delta_{a^{-1}}$; (iii) $T(G)$ é um subgrupo do grupo $(S(G), \circ)$ das permutações dos elementos de $G$.

*Demonstração:*

(i) Sejam $\delta_a$ e $\delta_b$ translações de $G$. Então:

$$(\delta_a \circ \delta_b)(x) = \delta_a(\delta_b(x)) = \delta_a(bx) = a(bx) = (ab)x = \delta_{ab}(x)$$

o que mostra que $\delta_a \circ \delta_b = \delta_{ab}$.

(II) Como $\delta_a$ é bijetora (proposição anterior), procede falar em aplicação inversa neste caso. E o enunciado já aponta a "candidata": a translação $\delta_{a^{-1}}$. Daqui para a frente é apenas uma questão de verificação:

• Como $(\delta_a \circ \delta_{a^{-1}})(x) = \delta_a(\delta_{a^{-1}}(x)) = \delta_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = x = i_G(x)$, então $\delta_a \circ \delta_{a^{-1}} = i_G$.

• Da mesma forma se prova que $\delta_{a^{-1}} \circ \delta_a = i_G$.

Portanto, efetivamente, $\delta_{a^{-1}}$ é a inversa de $\delta_a$, isto é, $(\delta_a)^{-1} = \delta_{a^{-1}}$.

(II') Sejam $\delta_a$ e $\delta_b \in T(G)$. Então:

$$\delta_a \circ (\delta_b)^{-1} = \delta_a \circ (\delta_{b^{-1}}) = \delta_{ab^{-1}}$$

De onde, $\delta_a \circ (\delta_b)^{-1} \in T(G)$ e, portanto, $T(G)$ é um subgrupo de $S(G)$. #

**Proposição 10** (teorema de Cayley): Se $G$ é um grupo, a aplicação $f: G \to T(G)$ que associa a cada elemento $a$ a translação $\delta_a$ (isto é, $f(a) = \delta_a$) é um isomorfismo de grupos.

*Demonstração:*

• Se $a, b \in G$ e $f(a) = f(b)$, então $\delta_a = \delta_b$. Portanto, $\delta_a(x) = \delta_b(x)$, qualquer que seja $x \in G$. Lembrando a definição de translação, temos que $ax = bx$, qualquer que seja $x \in G$. Em particular, para o elemento neutro $e$, $ae = be$, ou seja, $a = b$. Isso mostra que $f$ é injetora.

• Como uma translação é sempre do tipo $\delta_a$, com $a \in G$, então necessariamente $f$ é sobrejetora.

• Para quaisquer $a, b \in G$:

$$f(ab) = \delta_{ab} = \delta_a \circ \delta_b = f(a) \circ f(b)$$

e, portanto, $f$ é um homomorfismo de grupos. #

O teorema mostra que o grupo $T(G)$ é uma representação do grupo $G$. Como os elementos de $T(G)$ são particulares permutações dos elementos de $G$, então efetivamente todo grupo pode ser representado por um grupo de permutações dos elementos de $G$.

*Exemplo 18:* Consideremos o grupo aditivo $\mathbb{Z}_3$ das classes de resto módulo 3. Para facilitar a notação, deixaremos de colocar traços sobre os elemento de $\mathbb{Z}_3$. Portanto, $\mathbb{Z}_3 = \{0, 1, 2\}$ e a operação considerada é a adição módulo 3 (por exemplo, $2 + 2 = 1$). A tábua do grupo, sem os traços, fica assim:

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Para encontrar o modelo fornecido pelo teorema de Cayley para esse grupo indicaremos as permutações como em **2.4** (xii-b). Assim, a translação à esquerda definida por $a$, ou seja, a aplicação $\delta_a$ que associa a cada $x$ do grupo o elemento $a + x$ (lembrar que $\mathbb{Z}_3$ é aditivo), será denotada por:

$$\delta_a = \begin{pmatrix} 0 & 1 & 2 \\ a + 0 & a + 1 & a + 2 \end{pmatrix}$$

Portanto, as translações são:

$$\delta_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 + 0 & 0 + 1 & 0 + 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 + 0 & 1 + 1 & 1 + 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\delta_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 + 0 & 2 + 1 & 2 + 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

De onde:

$$T(\mathbb{Z}_3) = \left\{ \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \right\}$$

é o grupo de permutações que representa $\mathbb{Z}_3$, conforme o teorema de Cayley.

## Exercícios

**48.** Verifique em cada caso se $f$ é um homomorfismo:

a) $f: \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = kx$, sendo $\mathbb{Z}$ o grupo aditivo dos inteiros e $k$ um inteiro dado.

b) $f: \mathbb{R}^* \to \mathbb{R}^*$ dada por $f(x) = |x|$, sendo $\mathbb{R}^*$ o grupo multiplicativo dos reais.

c) $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x + 1$, sendo $\mathbb{R}$ o grupo aditivo dos reais.

d) $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(x) = (x, 0)$ em que $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ denotam grupos aditivos.

e) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por $f(x, y) = x$ em que $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ denotam grupos aditivos.

f) $f: \mathbb{Z} \to \mathbb{R}^*_+$ dada por $f(x) = 2^x$, em que $\mathbb{Z}$ é grupo aditivo e $\mathbb{R}^*_+$ é grupo multiplicativo.

**49.** Determine os homomorfismos injetores e sobrejetores do exercício 48.

**50.** Determine o núcleo de cada homomorfismo do exercício 48.

**51.** Seja $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dada pela lei $f(x, y) = (x - y, 0)$. Prove que $f$ é um homomorfismo do grupo aditivo $\mathbb{Z} \times \mathbb{Z}$ em si próprio. Obtenha $N(f)$.

**52.** Das aplicações a seguir, algumas são homomorfismos do grupo multiplicativo $\mathbb{C}^*$.

Descubra quais e determine o núcleo de cada uma.

a) $f(z) = z^2$

b) $f(z) = |z|$

c) $f(z) = z$

d) $f(z) = \frac{1}{z}$

e) $f(z) = -\frac{1}{z}$

f) $f(z) = -z$

g) $f(z) = z^3$

**53.** Prove que a aplicação $f: \mathbb{Z} \to \mathbb{C}^*$ dada por $f(n) = i^n$ é um homomorfismo do grupo aditivo $\mathbb{Z}$ no grupo multiplicação $\mathbb{C}^*$. Determine $N(f)$.

**54.** Sejam $G$ e $J$ grupos multiplicativos, $f$ um homomorfismo de $G$ em $J$ e $H$ um subgrupo de $J$. Mostre que $f^{-1}(H) = \{x \in G \mid f(x) \in H\}$ é um subgrupo de G.

**55.** Sejam $G$ um grupo multiplicativo comutativo e $n$ um número inteiro positivo. Mostre que a aplicação $f(x) = x^n$ é um homomorfismo de $G$.

**56.** Prove que um grupo $G$ é abeliano se, e somente se, $f: G \to G$ definida por $f(x) = x^{-1}$ é um homomorfismo.

**57.** Seja $\mathbb{R}^*$ o grupo multiplicativo dos números reais não nulos. Descreva explicitamente o núcleo do homomorfismo "valor absoluto" $x \mapsto |x|$ de $\mathbb{R}^*$ em si mesmo. Qual é a imagem desse homomorfismo?

**58.** Sejam os grupos $(G, \cdot)$ e $(J, \cdot)$ e seja $G \times J$ o produto direto de $G$ por $J$. Estabeleça quais das aplicações abaixo são homomorfismos e determine seus núcleos

a) $f_1: G \times J \to G$ dada por $f_1(x, y) = x$

b) $f_2: G \times J \to J$ dada por $f_2(x, y) = y$

c) $f_3: G \to G \times J$ dada por $f_3(x) = (x, 1)$

d) $f_4: G \times J \to J \times G$ dada por $f_4(x, y) = (y, x)$

e) $f_5: J \to G \times J$ dada por $f_5(y) = (1, y)$

**59.** Construa a tábua de um grupo $G = \{e, a, b, c\}$ que seja isoformo ao grupo multiplicativo $H = \{1, i, -1, -i\}$.

**60.** Construa a tábua do grupo multiplicativo $G = \{e, a, b, c\}$ de modo que $G$ seja isomorfo do grupo $(\mathbb{Z}_5^*, \cdot)$. Em seguida, resolva em $G$ a equação $axb^{-1} = c^2$.

**61.** Mostre que $G = \mathcal{P}(\{a, b\})$ com a operação diferença simétrica e o grupo $H = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ com a operação de multiplicação módulo 8 são isomorfos.

**62.** Mostre que se $G = \{e, a, b, c\}$ é um grupo, de ordem 4, com elemento neutro $e$, então só há duas possibilidades essencialmente distintas para a tábua de $G$.
*Sugestão:* Notar que $a * b = e$ ou $a * b = c$.
*Observação:* Um grupo $G = \{e, a, b, c\}$, de ordem 4, em que $a^2 = b^2 = c^2 = e$ (elemento neutro), chama-se *grupo de Klein*.

**63.** Mostre que o grupo de Klein, $G = \{e, a, b, c\}$, e o grupo aditivo $\mathbb{Z}_4$ não são isomorfos.
*Sugestão:* Tomar um possível homomorfismo $f: \mathbb{Z}_4 \to G$ e mostrar que $f$ não é bijetora.

**64.** Sabendo que $G = \{e, a, b, c, d, f\}$ é um grupo multiplicativo isomorfo do grupo aditivo $\mathbb{Z}_6$, faça o que se pede:

a) Construa uma tábua para $G$.
b) Calcule $a^2$, $b^{-2}$ e $c^{-3}$.
c) Obtenha $x \in G$ tal que $bxc = a^{-1}$.

**65.** Mostre que $f: \mathbb{Z} \to 2\mathbb{Z}$ dada por $f(n) = 2n, \forall n \in \mathbb{Z}$, é um isomorfismo do grupo aditivo $\mathbb{Z}$ no grupo aditivo $2\mathbb{Z}$.

**66.** Seja $a \in \mathbb{R}^*_+$ e $a \neq 1$.

a) Mostre que $G = \{a^n \mid n \in \mathbb{Z}\}$ é um subgrupo de $(\mathbb{R}^*_+, \cdot)$.
b) Mostre que $f: \mathbb{Z} \to G$ tal que $f(n) = a^n$ é um isomorfismo de $(\mathbb{Z}, +)$ em $(G, \cdot)$.

**67.** Prove que a função exponencial $f(x) = a^x$, com $0 < a \neq 1$, é um isomorfismo do grupo aditivo $\mathbb{R}$ no grupo multiplicativo $\mathbb{R}^*_+$.
Qual é o isomorfismo inverso?

**68.** Mostre que $G = \{2^m 3^n \mid m, n \in \mathbb{Z}\}$ e $J = \{m + ni \mid m, n \in \mathbb{Z}\}$ são subgrupos de $(\mathbb{R}^*, \cdot)$ e $(\mathbb{C}, +)$, respectivamente, e que são isomorfos.

**69.** Seja $\text{Aut}(G)$ o conjunto de todos os automorfismos de um grupo $G$ (isomorfismos de $G$ em $G$). Mostre que $(\text{Aut}(G), \circ)$ é um grupo.

**70.** Prove que se $G$ é um grupo não comutativo, então $\text{Aut}(G)$ também é não comutativo.

**71.** Determine todos os automorfismos do grupo de Klein.

**72.** Seja $a$ um elemento fixo do grupo $G$ (multiplicativo). Prove que $f: G \to G$ definida por $f(x) = axa^{-1}$ é um isomorfismo.

**73.** Mostre que há pelo menos dois homomorfismos e ao menos um isomorfismo de um grupo nele próprio.

**Exercício complementar**

**C4.** Mostre que $f$ é um isomorfismo do grupo aditivo dos racionais se, e somente se, existir $c \in \mathbb{Q}^*$ de modo que $f(x) = cx, \forall x \in \mathbb{Q}$.

# IV-3 GRUPOS CÍCLICOS

## 9. POTÊNCIAS E MÚLTIPLOS

Os conceitos de potência e múltiplo a serem introduzidos neste item são similares no que se refere a grupos. A diferença é apenas de notação. Enquanto o primeiro desses conceitos se refere a grupos multiplicativos, o segundo se refere a grupos aditivos. Por essa razão, basta desenvolver o assunto com uma das notações e o faremos com a multiplicativa, por ser mais simples e de uso mais frequente na teoria dos grupos. Ao final, enunciaremos a definição e as propriedades para o caso aditivo.

**Definição 7:** Seja $G$ um grupo multiplicativo. Se $a \in G$ e $m$ é um número inteiro, a *potência* m *ésima* de $a$, ou potência de $a$ de expoente $m$, é o elemento de $G$ denotado por $a^m$ e definido da seguinte maneira:

• se $m \geq 0$, por recorrência, da seguinte forma

$$a^0 = e \text{ (elemento neutro de G)}$$
$$a^m = a^{m-1}a, \text{ se } m \geqslant 1$$

• se $m < 0$

$$a^m = (a^{-m})^{-1}$$

A definição por recorrência no caso $m \geqslant 0$ deve ser interpretada assim: $a^1 = a^{1-1}a = a^0a = ea = a$; $a^2 = a^{2-1}a = a^1a = aa$; $a^3 = a^{3-1}a = a^2a = (aa)a$, etc.

Uma conseqüência imediata dessa definição é que, para todo inteiro $m$, vale $e^m = e$.

*Exemplo 19:* No grupo multiplicativo $GL_2(\mathbb{R})$ das matrizes reais $2 \times 2$ inversíveis, seja $A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$. Então:

$$A^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A^1 = A, A^2 = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 8 & 11 \end{pmatrix}, \ldots$$

$$A^{-1} = [1/\det(A)] \cdot \text{adj}(A) = \frac{1}{1} \cdot \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix},$$

$$A^{-2} = (A^2)^{-1} = \begin{pmatrix} 3 & 4 \\ 8 & 11 \end{pmatrix}^{-1} = \frac{1}{1}\begin{pmatrix} 11 & 4 \\ 8 & 3 \end{pmatrix} = \begin{pmatrix} 11 & 4 \\ 8 & 3 \end{pmatrix}, \ldots$$

*Exemplo 20:* No grupo multiplicativo $\mathbb{Z}_5^*$ das classes de resto módulo 5, seja $a = \bar{2}$. Então:

$$\bar{2}^0 = \bar{1}, \bar{2}^1 = \bar{2}, \bar{2}^2 = \bar{2} \cdot \bar{2} = \bar{4}, \bar{2}^3 = \bar{4} \cdot \bar{2} = \bar{3}, \ldots$$

$$\bar{2}^{-1} = \bar{3}, \bar{2}^{-2} = (\bar{2}^2)^{-1} = (\bar{4})^{-1} = \bar{4}, \ldots$$

*Exemplo 21:* No grupo $S_3$ das permutações dos elementos de $\{1, 2, 3\}$, seja $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Então:

$a^0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$; $a^1 = a$; $a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $a^3 = a^2a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$; ... (É importante observar que, neste caso, as potências de expoente positivo se repetem ciclicamente a partir desta ultima; ou seja, $a^4 = a^3 \circ a = e \circ a = a$; $a^5 = a^4 \circ a = a \circ a = a^2$; $a^6 = a^3$; etc.);

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; a^{-2} = (a^2)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \ldots$$

**Proposição 11:** Seja $G$ um grupo multiplicativo. Se $m$ e $n$ são números inteiros e $a \in G$, então:

(i) $a^m a^n = a^{m+n}$;

(ii) $a^{-m} = (a^m)^{-1}$;

(iii) $(a^m)^n = a^{mn}$.

*Demonstração:*

(i)

• Demonstraremos primeiro para o seguinte caso particular: $n \geqslant 0$ e $m + n \geqslant 0$. O raciocínio será por indução sobre $n$.

Se $n = 0$, então $a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$. Portanto, a propriedade é verdadeira quando $n = 0$. Seja $r \geqslant 0$ e suponhamos que, para qualquer inteiro $m$ tal que $m + r \geqslant 0$, se tenha $a^{m+r} = a^m a^r$. Então $a^m a^{r+1} \overset{*}{=} a^m(a^r a) = (a^m a^r)a \overset{**}{=} a^{m+r}a \overset{*}{=} a^{(m+r)+1}$. (Chamamos a atenção para o seguinte: nas passagens assinaladas com * usamos a definição de potência, o que é possível porque $r + 1 \geqslant 1$ e $m + r + 1 \geqslant 1$; e na passagem assinalada com ** usamos a hipótese de indução.)

• Para o caso geral, sejam $m$ e $n$ inteiros quaisquer. Tomemos um número inteiro $p > 0$ tal que $p + n > 0$ e $p + m + n > 0$, o que obviamente sempre é possível. Isso posto, observemos primeiro que, devido à definição, $a^p a^{-p} = a^p(a^p)^{-1} = e$.

Então:

$$a^{m+n} = a^{m+n}(a^p a^{-p}) = (a^{m+n}a^p)a^{-p} \overset{*}{=} a^{(m+n)+p}a^{-p} = a^{m+(n+p)}a^{-p} \overset{*}{=} (a^m a^{n+p})a^{-p} \overset{*}{=}$$
$$\overset{*}{=} [a^m(a^n a^p)]a^{-p} = [(a^m a^n)a^p]a^{-p} = (a^m a^n)(a^p a^{-p}) = (a^m a^n)e = a^m a^n$$

(Notar que nas passagens assinaladas com * usamos a conclusão anterior.)

(ii) Observemos que, devido a (i), $a^{-m}a^m = a^{(-m)+m} = a^0 = e$; analogamente, $a^m a^{-m} = e$. Portanto, cada uma dessas potências é inversa da outra. Logo, $a^{-m} = (a^m)^{-1}$.

(iii) O caso em que $n \geqslant 0$ se demonstra por indução sobre $n$ e deixamos como exercício. Suponhamos $n < 0$. Então:

$$(a^m)^n \overset{*}{=} [(a^m)^{-n}]^{-1} = (a^{-mn})^{-1} \overset{**}{=} a^{mn}$$

(Na passagem assinalada com * usamos a definição; na assinalada com ** usamos (ii).) #

Um corolário imediato dessa proposição é que duas potências quaisquer de um mesmo elemento do grupo comutam entre si. Isto é, se $a \in G$ e $m, n \in \mathbb{Z}$, então $a^m a^n = a^n a^m$.

**Definição 8:** Seja $G$ um grupo aditivo. Se $a \in G$ e $m$ e um número inteiro, o *múltiplo* m *ésimo* de $a$ é o elemento de $G$ denotado por $m \cdot a$ e definido da seguinte maneira:

- se $m \geqslant 0$, por recorrência, da seguinte forma

$$0 \cdot a = e \text{ (elemento neutro de } G\text{)}$$
$$m \cdot a = (m - 1) \cdot a + a, \text{ se } m \geqslant 1$$

- se $m < 0$

$$m \cdot a = -[(-m) \cdot a]$$

*Exemplo 22:* No grupo aditivo $M_2(\mathbb{R})$ das matrizes reais $2 \times 2$, seja $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Então:

$0 \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; $1 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$; $2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} =$
$= \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$; $3 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 9 & 12 \end{pmatrix}$; ...
$(-1) \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = -\left[1 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\right] = \begin{pmatrix} -1 & -2 \\ -3 & -4 \end{pmatrix}$; $(-2) \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = -\left[2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\right] =$
$= -\begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix} = \begin{pmatrix} -2 & -4 \\ -6 & -8 \end{pmatrix}$; ... .

**Proposição 12:** Seja $G$ um grupo aditivo. Se $m$ e $n$ são números inteiros e $a \in G$, então:

(i) $m \cdot a + n \cdot a = (m + n) \cdot a$;

(ii) $(-m) \cdot a = -(m \cdot a)$;

(iii) $n \cdot (m \cdot a) = (nm) \cdot a$. #

## 10. GRUPOS CÍCLICOS

Se $a$ é elemento de um grupo multiplicativo $G$, denotaremos por $[a]$ o subconjunto de $G$ formado pelas potências inteiras de $a$, ou seja, $[a] = \{a^m \mid m \in \mathbb{Z}\}$. Esse subconjunto de $G$ nunca é vazio, pois $e$, o elemento neutro de $G$, pertence a ele, uma vez que $e = a^0$.

**Proposição 13:** (i) O subconjunto $[a]$ é um subgrupo de $G$; (ii) se $H$ é um subgrupo de $G$ ao qual $a$ pertence, então $[a] \subset H$.

*Demonstração:*

(i) Como já observamos, $[a] \neq \varnothing$. Sejam pois $u$ e $v$ elementos de $[a]$. Então $u = a^m$ e $v = a^n$, para convenientes inteiros $m$ e $n$. Daí, $uv^{-1} = a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n}$. Isso mostra que $uv^{-1} \in [a]$. De onde, $[a]$ é um subgrupo de $G$.

(ii) Se $a \in H$, então toda potência de $a$ também pertence a $H$ e, portanto, $[a] \subset H$. $\#$

A segunda parte dessa proposição nos diz, em outras palavras, que $[a]$ é o "menor" subgrupo de $G$ que inclui o elemento $a$

**Definição 9:** Um grupo multiplicativo $G$ será chamado *grupo cíclico* se, para algum elemento $a \in G$, se verificar a igualdade $G = [a]$ Nessas condições, o elemento $a$ é chamado *gerador* do grupo $G$.

Então, dizer que um grupo multiplicativo $G$ é *cíclico* significa dizer que $G = \{a^m \mid m \in \mathbb{Z}\}$, para algum $a \in G$. E no caso aditivo significa, ajeitando-se a notação, que $G$ inclui um elemento $a$ tal que $G = \{m \cdot a \mid m \in \mathbb{Z}\} = \{..., (-2) \cdot a, -a, e = 0 \cdot a, a, 2 \cdot a, ...\}$. O fato de $m$ ser variável no conjunto $\mathbb{Z}$, que é infinito, não quer dizer que $[a]$ seja infinito, como será visto. Como veremos, também, um grupo cíclico pode ter mais do que um gerador.

*Exemplo 23:* No grupo multiplicativo $\mathbb{C}^*$, encontrar o subgrupo gerado por $i$. Por definição, $[i] = \{i^m \mid m \in \mathbb{Z}\}$. Mas, como se vê no estudo dos números complexos, esse conjunto só tem 4 elementos, $1, i, -1, -i$, obtidos respectivamente quando $m = 4q$, $m = 4q + 1$, $m = 4q + 2$ e $m = 4q + 3$. Portanto, $[i] = \{1, -1, i, -i\}$. É oportuno, nesta altura, mostrar a tábua desse grupo:

| $\cdot$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| **$1$** | $1$ | $-1$ | $i$ | $-i$ |
| **$-1$** | $-1$ | $1$ | $-i$ | $i$ |
| **$i$** | $i$ | $-i$ | $-1$ | $1$ |
| **$-i$** | $-i$ | $i$ | $1$ | $-1$ |

*Exemplo 24:* Seja $n > 1$ um número inteiro O conjunto das raízes $n$-ésimas da unidade é um subgrupo do grupo multiplicativo $\mathbb{C}^*$ e é cíclico. De fato:

• Sejam $\alpha$, $\beta$ raízes $n$-ésimas da unidade. Então $\alpha^n = 1$ e $\beta^n = 1$ e, daí, $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = 1 \cdot 1^{-1} = 1$. Portanto, trata-se de um subgrupo de $\mathbb{C}^*$

• O conjunto das raízes $n$-ésimas da unidade é:

$$\{\cos[(2k\pi)/n] + i\,\text{sen}[(2k\pi)/n] \mid k = 0, 1, 2, ..., n - 1\}$$

Observe-se que $\tau_n = \cos[(2\pi)/n] + i\,\text{sen}[(2\pi)/n]$ gera todas as raízes, pois $\tau_n^k = \cos[(2k\pi)/n] + i\,\text{sen}[(2k\pi)/n]$. Uma raiz, como $\tau_n$, geradora do grupo multiplicativo das raízes da unidade, chama-se *raiz primitiva* n*-ésima da unidade*

*Exemplo 25:* No grupo $S_3$, encontrar o subgrupo gerado por $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Observemos que $f_1^0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_0$ (elemento neutro), $f_1^1 = f_1$, $f_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ$ $\circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$, $f_1^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} =$

$= f_0$, $f_1^4 = f_1$, $f_1^5 = f_2$, $f_1^6 = f_0$, ... . (Notar que as permutações $f_0$, $f_1$ e $f_2$ se repetem ciclicamente.)

Por outro lado:

$f_1^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$, $f_1^{-2} = (f_1^2)^{-1} = f_2^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_1$, $f_1^{-3} = (f_1^3)^{-1} =$ $= f_0^{-1} = f_0$, $f_1^{-4} = f_2$, $f_1^{-5} = f_1$, ... . (Notar que também aqui há repetição cíclica de $f_0$, $f_1$ e $f_2$.)

Portanto, $[f_1] = \{f_0, f_1, f_2\}$.

Mais à frente, com a teoria a ser desenvolvida, teremos condições, em casos como esse, de determinar os elementos do grupo cíclico sem precisar fazer tantos "cálculos". Convém observar ainda que, repetindo esse raciocínio para os demais elementos do grupo (exercício que recomendamos aos estudantes), encontraríamos o seguinte: $[f_0] = \{f_0\}$; $[f_2] = \{f_0, f_1, f_2\}$; $[g_1] = \{f_0, g_1\}$; $[g_2] = \{f_0, g_2\}$; $[g_3] = \{f_0, g_3\}$. Isso mostra que $S_3$ não é gerado por nenhum de seus elementos e, portanto, que não é um grupo cíclico.

*Exemplo 26:* O grupo aditivo $\mathbb{Z}$ é cíclico, pois todos os seus elementos são múltiplos de 1 ou de $-1$. De fato, $\mathbb{Z} = \{m \cdot 1 \mid m \in \mathbb{Z}\}$ ou $\mathbb{Z} = \{m \cdot (-1) \mid m \in \mathbb{Z}\}$. Portanto, $\mathbb{Z} = [1] = [-1]$. Os números 1 e $-1$ são, na verdade, os únicos geradores de $\mathbb{Z}$.

**Proposição 14:** Todo subgrupo de um grupo cíclico é também cíclico.

*Demonstração:* A demonstração será feita, mais uma vez, com a notação multiplicativa, e o elemento neutro do grupo será denotado por $e$. Assim, se $H$ é um subgrupo do grupo cíclico $G = [a]$, então todo elemento de $H$ é do tipo $a^m$, para algum inteiro $m$, pois também é um elemento de $G$.

Suponhamos que $H = \{a^0\} = \{e\}$. Nesse caso, $H$ é cíclico gerado por $a^0 = e$, pois qualquer potência de $e$ é igual ao próprio $e$.

Caso contrário, $H$ inclui um elemento $a^m$ cujo expoente é diferente de zero. Mas como $(a^m)^{-1} = a^{-m} \in H$, então pode-se dizer que, neste caso, $H$ possui um elemento de expoente estritamente positivo. Seja $h$ o menor inteiro estritamente positivo para o qual $a^h \in H$. Mostraremos que $b = a^h$ gera $H$, ou seja, que $H = [b]$. Para isso, tomemos um elemento genérico $x = a^n \in H$. O algoritmo euclidiano usado com $n$ como dividendo e $h$ como divisor garante que se podem encontrar dois inteiros $q$ e $r$ tais que

$$n = hq + r \; (0 \leqslant r < h)$$

Portanto:

$$x = a^n = a^{hq+r} = (a^h)^q a^r$$

Daí:

$$a^r = (a^h)^{-q} x = b^{-q} x$$

Como, porém, $(b)^{-q} \in H$ (porque $b \in H$) e $x \in H$ (por hipótese), então $a^r \in H$ (por ser o produto de dois elementos de $H$). Portanto, não se pode ter $r > 0$, pois isso implicaria a existência de um elemento em $H$ de expoente estritamente positivo e menor que $h$, o que não é possível. Então $r = 0$ e

$$x = a^n = a^{hq} = (a^h)^q = b^q$$

e, portanto, $x \in [b] = [a^h]$. Esse raciocínio mostra que $H \subset [b]$. Mas também vale a inclusão contrária, pois, se $b \in H$, o mesmo se pode dizer de qualquer potência de $b$. De onde, $H = [b]$. #

*Exemplo 27:* Devido à proposição anterior, pode-se garantir que um subconjunto não vazio $H \subset \mathbb{Z}$ é um subgrupo de $(\mathbb{Z}, +)$ se, e somente se, $H = [m]$, para algum inteiro $m \in H$. Portanto, os subgrupos de $\mathbb{Z}$ são:

$[0] = \{0\}$, $[1] = [-1] = \mathbb{Z}$, $[2] = [-2] = \{0, \pm 2, \pm 4, ...\}$, $[3] = [-3] = \{0, \pm 3, \pm 6, ...\}$, etc.

## 11. CLASSIFICAÇÃO DOS GRUPOS CÍCLICOS

Seja $G = [a]$ um grupo cíclico. Dois casos podem ocorrer:

*Caso 1:* $a^r \neq a^s$ sempre que $r \neq s$.

Um exemplo que se enquadra nessa exigência é o subgrupo $G$ gerado pelo número 2 no grupo multiplicativo $\mathbb{Q}^*$, ou seja, $G = [2] = \{..., 2^{-2}, 2^{-1}, 2^0 = 1, 2^1, 2^2, ...\}$.

Nesse exemplo, chama a atenção a seguinte aplicação de $\mathbb{Z}$ em $[2]$:

$$\begin{array}{cccccccc} ..., & -2, & -1, & 0, & 1, & 2, & ..., & r, & ... \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \\ ..., & 2^{-2}, & 2^{-1}, & 2^0 = 1, & 2^1, & 2^2, & ..., & 2^r, & \end{array}$$

No caso geral de um grupo cíclico $G = [a]$, ela é definida por $r \mapsto a^r$ e tem, como veremos, um papel fundamental no que se refere à representação dos grupos enquadrados neste caso. Com vistas a estudar esse papel, denotaremos essa aplicação por $f$

Portanto, $f: \mathbb{Z} \to G = [a]$ é a aplicação assim definida: $f(r) = a^r$.

• Devido à própria definição dos grupos cíclicos do caso em estudo, ou seja, $a^r \neq a^s$ sempre que $r \neq s$, a aplicação $f$ é injetora.

• Ela também é sobrejetora, porque todo elemento de $y \in G$ pode ser escrito como $y = a^r$, para algum inteiro $r$, e, para esse elemento, $f(r) = a^r = y$.

• E é um homomorfismo do grupo aditivo $\mathbb{Z}$ no grupo $G$. De fato:

$$f(m + n) = a^{m+n} = a^m a^n = f(m)f(n)$$

Portanto, acabamos de demonstrar a seguinte proposiçao.

**Proposição 15:** Se $G = [a]$ é um grupo cíclico que cumpre a condiçao do caso 1, então a aplicação $f: \mathbb{Z} \to G$ definida por $f(r) = a^r$ é um isomorfismo de grupos.

O fato de a aplicação $f$ ser uma bijeção tem como conseqüência que os conjuntos $\mathbb{Z}$ e $G = [a]$ têm a mesma cardinalidade e, portanto, $G$ é infinito. Por essa razão, os grupos que se enquadram no caso 1 são chamados *grupos cíclicos infinitos*. No aspecto algébrico, o fato de $f$ ser um isomorfismo leva à conclusão de que todos os grupos cíclicos infinitos são cópias do grupo aditivo $\mathbb{Z}$.

*Caso 2:* $a^r = a^s$ para algum par de inteiros distintos, $r$ e $s$.

Suponhamos $r > s$. Então $a^r(a^s)^{-1} = a^s(a^s)^{-1} = e$ e, daí, $a^{r-s} = e$, em que $r - s > 0$. Isso mostra que há potências de $a$, com expoentes estritamente positivos, iguais ao elemento neutro $e$. Portanto, é possível fazer a seguinte escolha: seja $h$ o menor número inteiro estritamente positivo e tal que $a^h = e$.

Então $a^h = e$, $a^{h+1} = a^h a = ea = a$, $a^{h+2} = a^{h+1}a = aa = a^2$, ... . Ou seja, a partir do expoente $h$ as potências de $a$ se repetem ciclicamente. Uma primeira pergunta que surge é se na seqüência de potências $a^0 = e, a^1 = a, a^2, \ldots, a^{h-1}$ há elementos repetidos. A resposta é negativa. De fato, suponhamos $a^i = a^j$, com $0 \leqslant i < j < h$. Então $0 < j - i < h$ e $a^{j-i} = a^j(a^i)^{-1} = a^j(a^j)^{-1} = e$. Mas isso é absurdo, porque, dada a escolha de $h$, não se pode ter simultaneamente $0 < j - i < h$ e $a^{j-i} = e$.

A segunda pergunta é se há outros elementos no grupo além de $e, a, a^2, \ldots, a^{h-1}$. A resposta também é negativa. De fato, seja $x$ um elemento de $G = [a]$. Então, $x = a^m$ para algum inteiro $m$. Usando-se o algoritmo euclidiano com $m$ como dividendo e $h$ como divisor:

$$m = hq + r \ (0 \leqslant r < h)$$

Então:

$$a^m = a^{hq+r} = (a^h)^q a^r = e^q a^r = ea^r = a^r$$

Como os valores possíveis de $r$ são $0, 1, 2, \ldots, h - 1$, então as possibilidades para $a^m$ são $a^0 = e, a^1 = a, a^2, \ldots, a^{h-1}$. Isso mostra que $[a] \subset \{a^0 = e, a^1 = a, a^2, \ldots, a^{h-1}\}$. Obviamente, porém, devido à definição de $[a]$, vale a inclusão contrária. De onde, $[a] = \{a^0 = e, a^1 = a, a^2, \ldots, a^{h-1}\}$ e a ordem desse grupo é $h$.

Demonstramos, pois, a seguinte proposição.

**Proposição 16:** Seja $G = [a]$ um grupo cíclico que cumpre as condiçoes do caso 2. Então existe um inteiro $h > 0$ tal que: (i) $a^h = e$; (ii) $a^r \neq e$ sempre que $0 < r < h$. Neste caso, a ordem do grupo é $h$ e

$$G = [a] = \{e, a, a^2, ..., a^{h-1}\}$$

Como não poderia deixar de ser, o grupo, neste caso, é chamado *grupo cíclico finito*, e o expoente $h$, com o significado das considerações anteriores, *período* ou *ordem* de $a$. Em suma, o período de um elemento $a$ de um grupo é um inteiro $h > 0$ se: (i) $a^h = e$; (ii) $a^r \neq e$, qualquer que seja o inteiro $r$ sujeito às restrições $0 < r < h$. É claro que, neste caso, $a$ gera um grupo de ordem $h$.

Se, para qualquer inteiro $r \neq 0$, $a^r \neq e$, então se diz que a *ordem* ou *período* de $a$ é *zero*. Se a ordem de um elemento de um grupo é zero, então ele gera um subgrupo cíclico infinito. De fato, neste caso não se pode ter $m \neq n$ e $a^m = a^n$, pois, supondo, por exemplo, $m > n$, então $a^{m-n} = e$, o que é impossível, devido à suposição feita.

De modo geral, o período de um elemento $a$ de um grupo é denotado por $o(a)$.

*Exemplo 28:* O período de 1 no grupo multiplicativo dos números complexos é 1, uma vez que $1^1 = 1$, o período de $-1$ é 2, porque $(-1)^1 = -1$ e $(-1)^2 = 1$, e o período de $i$ é 4, pois $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$ e $i^4 = 1$. Nesse mesmo grupo, o período do número $-i$ também é 4, como é fácil ver.

Os números $1, -1, i, -i$ considerados são as raízes quárticas da unidade. Como vimos, duas delas, $i$ e $-i$, as raízes primitivas, têm período 4 e, portanto, cada uma delas gera o grupo das raízes quárticas. De modo geral, como já vimos (exemplo 24), o conjunto das raízes $n$-ésimas da unidade é um subgrupo de $\mathbb{C}^*$ e é cíclico. Qualquer dos seus geradores, ou seja, qualquer raiz primitiva $n$-ésima da unidade, como $\tau_n = \cos(2\pi/n) + i\text{sen}(2\pi/n)$, por exemplo, tem período $n$.

Ainda no grupo multiplicativo $\mathbb{C}^*$, o elemento $2i$, por exemplo, tem ordem *zero*, uma vez que $(2i)^n = 2^n i^n = 2^n, -2^n, 2^n i$ ou $-2^n i$ e nenhum número desse tipo é igual a 1.

**Proposição 17:** Seja $a$ um elemento de período $h > 0$ de um grupo $G$. Então $a^m = e$ se, e somente se, $h \mid m$.

*Demonstração:*

$(\rightarrow)$ A idéia aqui é usar o algoritmo euclidiano com $m$ como dividendo e $h$ como divisor:

$$m = hq + r \ (0 \leq r < h)$$

Então:

$$e = a^m = a^{hq+r} = a^{hq}a^r = (a^h)^q a^r = e^q a^r = ea^r = a^r$$

Ou seja, $a^r = e$. Como não se pode ter $r > 0$, pois isso contraria a hipótese de que o período de $a$ é $h$, então $r = 0$ e, portanto, $m = hq$. De onde, $h \mid m$.

(⟸) Se $h \mid m$, então $m = hq$, para algum $q \in \mathbb{Z}$. Então, $a^m = a^{hq} = (a^h)^q = e^q = e$. #

**Proposição 18:** Seja $G = [a]$ um grupo cíclico finito de ordem $h$. Então: (i) a correspondência $s \mapsto a^s$ é uma aplicação de $\mathbb{Z}_h$ em $G$; (ii) essa aplicação é um isomorfismo do grupo $(\mathbb{Z}_h, +)$ no grupo $(G, \cdot)$.

*Demonstração:*

(i) Nesta parte temos de demonstrar que nenhum elemento de $\mathbb{Z}_h$ tem dois associados em $G$, ou seja, que a duas representações de um mesmo elemento de $\mathbb{Z}_h$ está associado, pela correspondência definida, o mesmo elemento de $G$. De fato, suponhamos $\bar{r} = \bar{t}$. Então, $r - t = hq$ para um conveniente inteiro $q$. Daí:

$$a^r = a^{t + hq} = a^t a^{hq} = a^t (a^h)^q = a^t e^q = a^t e = a^t$$

Portanto, se $\bar{r} = \bar{t}$, então $a^r = a^t$.

(ii) Seja $f: \mathbb{Z}_h \to G$ definida por $f(\bar{r}) = a^r$.

• Se $a^r = a^s$, então $a^{r - s} = e$ e então, devido à proposição anterior, $r - s = hq$, para algum inteiro $q$. Daí $r \equiv s \pmod h$ e, portanto, $\bar{r} = \bar{s}$. Isso mostra que $f$ é injetora.

• Seja $y \in G$. Então, $y = a^r$ para algum inteiro $r$, sujeito às restrições $0 \leq r < h$. De onde, $\bar{r} \in \mathbb{Z}_h$ e

$$f(\bar{r}) = a^r = y$$

Fica provado, pois, que $f$ também é sobrejetora.

• Por fim, sejam $\bar{r}, \bar{s} \in \mathbb{Z}_h$. Então:

$$f(\bar{r} + \bar{s}) = f(\overline{r + s}) = a^{r + s} = a^r a^s = f(\bar{r}) + f(\bar{s})$$

e, portanto, $f$ é um homomorfismo de grupos. Juntando tudo, conclui-se que $f$ é um isomorfismo de grupos, como queríamos provar. #

Essa proposição nos dá conta de que o grupo aditivo $\mathbb{Z}_h$ é uma cópia aditiva de todos os grupos cíclicos finitos de ordem $h$. Igualmente, o grupo das raízes $h$-ésimas da unidade é uma cópia multiplicativa.

## 12. GRUPOS DE TIPO FINITO

Seja $(G, \cdot)$ um grupo e $L = \{a_1, a_2, ..., a_n\}$ um subconjunto de $G$. Considerando que a coleção dos subgrupos de $G$ que contém $L$ não é vazia (pelo menos $G$ pertence a ela), a questão que nos propomos é a seguinte: qual o menor subgrupo de $G$ que contém $L$?

Para responder a essa pergunta, procuraremos generalizar o que foi feito para subgrupos cíclicos. Denotemos por $[L]$ o conjunto de todos os elementos de $G$ que se podem expressar da seguinte maneira: $x_1^{m_1}, x_2^{m_2} ... x_r^{m_r}$, em que $x_1, x_2, ..., x_r \in L$ e os expoentes são inteiros. Provemos primeiro que $[L]$ é um subgrupo de $G$.

De fato, se $u, v \in [L]$, então $u = x_1^{m_1}, x_2^{m_2} ... x_r^{m_r}$ e $v = y_1^{n_1}, y_2^{n_2} ... y_t^{n_t}$, para convenientes elementos $x_1, x_2, ..., x_r, y_1, y_2, ..., y_t \in L$ e expoentes inteiros. Daí:

$$uv^{-1} = x_1^{m_1} x_2^{m_2} \dots x_r^{m_r} y_t^{-n_t} y_{t-1}^{-n_{t-1}} \dots y_1^{-n_1}$$

expressão que nos autoriza a afirmar que $uv^{-1} \in [L]$, pois nas potências do segundo membro as bases são elementos de $L$ e os expoentes são inteiros.

Por outro lado, seja $H$ um subgrupo de $G$ que contém $L$. Mostraremos que $H \supset [L]$, o que completará nossa resposta à questão inicial. Para isso, tomemos $u \in [L]$. Então $u = x_1^{m_1} x_2^{m_2} \dots x_r^{m_r}$, com $x_1, x_2, \dots, x_r \in L$ e expoentes inteiros. Como pertencem a L, os elementos $x_1, x_2, \dots, x_r$ também pertencem a $H$. E, como $H$ é um subgrupo de G, então $x_1^{m_1}, x_2^{m_2}, \dots, x_r^{m_r} \in H$. Pelo mesmo motivo, também pertence a $H$ o produto desses elementos, ou seja, $u \in L$. Se todo elemento de $[L]$ é também elemento de $H$, então efetivamente, nas condições enunciadas, $[L] \subset H$.

O subgrupo $[L]$ assim definido é chamado *subgrupo de tipo finito gerado por* $L$. Um grupo $G$ se diz de *tipo finito* se existe $L \subset G$, $L$ finito, e tal que $[L] = G$.

*Exemplo 29:* Um grupo cíclico $G = [a]$ obviamente é de tipo finito. Neste caso, mantida a notação das considerações anteriores, $L = \{a\}$.

*Exemplo 30:* O produto direto de dois grupos cíclicos $G = [a]$ e $H = [b]$ é de tipo finito. De fato, se $L = \{(a, 1), (1, b)\}$, em que, por simplicidade, o símbolo 1 indica tanto o elemento neutro de $G$ como o de $H$, então $G \times H = [L]$. Para mostrar isso, basta observar que, para todo elemento $(a^m, b^n) \in G \times H$, vale a igualdade

$$(a^m, b^n) = (a, 1)^m (1, b)^n$$

*Exemplo 31:* O grupo $S_3$ das permutações dos elementos de $\{1, 2, 3\}$ é de tipo finito. De fato, como já vimos em **2.4** (xii-b), se

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

então $S_3 = \{f_1^0, f_1, f_1^2, g_1, g_1 f_1, g_1 f_1^2\}$, em que se adotou a notação multiplicativa em lugar da usada normalmente para a composição de aplicações. Essa maneira de escrever os elementos de $S_3$ mostra que, se $L = \{f_1, g_1\}$, então $S_3 = [L]$.

## Exercícios

**74.** Construa os seguintes subgrupos:

a) $[-1]_+$ em $(\mathbb{Q}, +)$

b) $[3]_+$ em $(\mathbb{Z}, +)$

c) $[3]$ em $(\mathbb{Q}^*, \cdot)$

d) $[i]$ em $(\mathbb{C}^*, \cdot)$

**75.** Mostre que todo grupo de ordem 2 ou 3 é cíclico.

**76.** Ache um grupo de ordem 4 cíclico e um não cíclico.

**77.** Mostre que os elementos não nulos de $\mathbb{Z}_{13}$ formam um grupo multiplicativo cíclico isomorfo ao grupo aditivo $\mathbb{Z}_{12}$.

**78.** Mostre que $(\mathbb{Z}_m, +)$ é cíclico, $\forall m > 1$.

**79.** Mostre que todo grupo cíclico infinito tem dois, e somente dois, geradores.

**80.** Mostre que todo subgrupo $H \neq \{e\}$ de um grupo cíclico infinito é também infinito.

**81.** A tábua ao lado define uma operação $\cdot$ que confere ao conjunto $E = \{e, a, b, c, d, f\}$ uma estrutura de grupo.

Pede-se determinar:

a) o subgrupo gerado por $b$;

b) o período de $d$;

c) os geradores de $G$;

d) $x \in G$ tal que $bxc = d^{-1}$.

| $\cdot$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $f$ | $e$ |
| $b$ | $b$ | $c$ | $d$ | $f$ | $e$ | $a$ |
| $c$ | $c$ | $d$ | $f$ | $e$ | $a$ | $b$ |
| $d$ | $d$ | $f$ | $e$ | $a$ | $b$ | $c$ |
| $f$ | $f$ | $e$ | $a$ | $b$ | $c$ | $d$ |

**Resolução**

a) $b^0 = e$, $b^1 = b$, $b^2 = d$, $b^3 = b^2b = db = e$

$[b] = \{e, b, d\}$

b) $d^0 = e$, $d^1 = d$, $d^2 = b$, $d^3 = e$

Então, $o(d) = 3$

c) Já sabemos que $e$, $b$, $d$ não são geradores de $G$. Por outro lado

$[a] = \{e, a, b, c, d, f\} = [f]$

$[c] = \{e, c\}$

Portanto, os geradores de $G$ são $a$ e $f$.

d) $bxc = d^{-1} \Leftrightarrow b^{-1}bxcc^{-1} = b^{-1}d^{-1}c^{-1} \Leftrightarrow x = b^{-1}d^{-1}c^{-1}$ então $x = dbc = ec = c$. ■

**82.** Seja $G = \{e, a, b, c, d, f, g, h\}$ um grupo cuja tábua é mostrada abaixo.

Pede-se determinar:

a) o subgrupo gerado por $b$;

b) o período de $d$;

c) os geradores de $G$;

d) $x \in G$ tal que $a \cdot x \cdot b^{-1} = d$.

| $\cdot$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ | $g$ | $h$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ | $g$ | $h$ |
| $a$ | $a$ | $d$ | $c$ | $g$ | $f$ | $e$ | $h$ | $b$ |
| $b$ | $b$ | $h$ | $d$ | $a$ | $g$ | $c$ | $e$ | $f$ |
| $c$ | $c$ | $b$ | $f$ | $d$ | $h$ | $g$ | $a$ | $e$ |
| $d$ | $d$ | $f$ | $g$ | $h$ | $e$ | $a$ | $b$ | $c$ |
| $f$ | $f$ | $e$ | $h$ | $b$ | $a$ | $d$ | $c$ | $g$ |
| $g$ | $g$ | $c$ | $e$ | $f$ | $b$ | $h$ | $d$ | $a$ |
| $h$ | $h$ | $g$ | $a$ | $e$ | $c$ | $b$ | $f$ | $d$ |

**83.** Sejam $m \in \mathbb{Z}, m > 1$. Indicando por $G_m$ o conjunto das raízes $m$-ésimas complexas de 1, mostre que $(G_m, \cdot)$ é um subgrupo cíclico de $(\mathbb{C}^*, \cdot)$.

**84.** Sejam $a$ e $b$ elementos de um grupo multiplicativo $G$. Supondo $o(ab) = h > 0$, mostre que $o(ba) = h$

**Resolução**

Se $o(a, b) = h > 0$, temos:

$(ab)^h = e$ e $(ab)^i \neq e$, $i \in \{1, 2, \ldots, h - 1\}$

Temos, por outro lado:

1º) $(ba)^h = b(ab)^{h-1}a = b(ab)^{-1}a = bb^{-1}a^{-1}a = e$

2º) Se $i \in \{1, 2, \ldots, h - 1\}$ e $(ba)^i = e$, decorre:

$b(ab)^{i-1}a = e \therefore (ab)^{i-1} = b^{-1}a^{-1} \therefore (ab)^{i-1} = (ab)^{-1}$

Isto é, $(ab)^i = e$, e isso é absurdo. ■

**85.** Mostre que o único elemento de um grupo de ordem 1 é o elemento neutro.

**86.** Seja $a \neq e$ um elemento do grupo $G$. Prove que $o(a) = 2$ se, e somente se, $a = a^{-1}$.

**87.** Seja $G$ um grupo finito de ordem par. Mostre que o número de elementos de $G$ de ordem 2 é ímpar.

**88.** Seja $G$ um grupo multiplicativo e $x \in G$. Mostre que, se existe um inteiro $n$, $n \geqslant 1$, tal que $x^n = e$, então existe um inteiro $m \geqslant 1$ tal que $x^{-1} = x^m$.

**89.** Se $a$, $b$ e $ab$ do grupo multiplicativo $G$ têm ordem 2, então $ab = ba$. Prove.

**90.** Seja $G$ um grupo multiplicativo e suponha $a \in G$. Mostre que $o(a) = o(a^{-1}) = o(xax^{-1})$, $\forall x \in G$.

**91.** Seja $G$ um grupo finito. Se $x \in G$, mostre que $\exists n \in \mathbb{Z}$ de modo que $x^n = e$ (elemento neutro).

**92.** Seja $G = [a]$ um grupo cíclico de ordem $h$. Mostre que $a^t \in G$ é um gerador de $G$ se, e somente se, $\text{mdc}(h, t) = 1$.

**Resolução**

($\Rightarrow$)

Se $a^t$ é um gerador de $G$, como $a \in G$, temos

$\exists r \in \mathbb{N} \mid (a^t)^r = a \therefore a^{tr} = a \therefore tr \equiv 1 \pmod{h} \therefore tr = 1 + kh \therefore 1 = tr - kh$

Seja $d = \text{mdc}(h, t)$. Então

$$\left.\begin{array}{l} d \mid t \Rightarrow d \quad tr \\ d \mid h \Rightarrow d \quad kh \end{array}\right\} \Rightarrow d \quad tr \quad kh \Rightarrow d \mid 1 \Rightarrow d \quad 1$$

$(\Leftarrow$

Se $1 - \text{mdc}(h, t)$, então existem dois inteiros $r$ e $s$ tais que $1 \quad rt + hs$ e, daí, $rt \quad 1$ (mod $h$); portanto, $a^{rt} = a$.

Dado $x \in G$, temos:

$x = a \ = (a^{rt})^{l} = (a^{t})^{r l}$

o que prova que $a^{t}$ é gerador de $G$. ∎

**93.** Mostre que todo subgrupo de um grupo cíclico é também cíclico.

**94.** Se $G = [a]$ é um grupo cíclico de ordem $h > 0$ e se $d$ é um divisor positivo de $h$, mostre que, sendo $t = h : d$, então $[a^t]$ é um subgrupo cíclico de $G$ de ordem $d$.

**95.** a) Defina subgrupo gerado por um subconjunto de elementos de um grupo aditivo.

b) Mostre que $(\mathbb{Z}^n, +)$ é de tipo finito $\forall n \geqslant 1$.
($\mathbb{Z}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{Z}\}$ é grupo aditivo)

**96.** Mostre que $(\mathbb{Q}, +)$ não é de tipo finito.

**97.** Seja $S$ uma parte não vazia de um grupo multiplicativo $G$. Mostre que todo subgrupo de $G$ que contém $S$ também contém $[S]$.

**98.** Seja $G - [a]$ um grupo cíclico de ordem $s$ e seja $G' - [b]$ um grupo cíclico de ordem $t$. Demonstre que existe um homomorfismo $\varphi$, de $G$ em $G'$, tal que $\varphi(a) = b^k$ se, e somente se, $sk$ é um múltiplo de $t$.

# IV-4 CLASSES LATERAIS — TEOREMA DE LAGRANGE

## 13. CLASSES LATERAIS

Consideremos, a título de motivação para o conceito a ser introduzido aqui, um subgrupo não trivial $H$ do grupo aditivo $\mathbb{Z}$. Como já vimos, $H$ necessariamente é cíclico, ou seja, $H$ possui um elemento $n > 1$ tal que $H = [n] = \{0, \pm n, \pm 2n, \dots\}$. Observemos então que, quaisquer que sejam $a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{n} \text{ se, e somente se, } a - b \in H$$

fato esse que estabelece uma correspondência entre subgrupos de $\mathbb{Z}$ e as relações de congruência, módulo $n$, sobre $\mathbb{Z}$.

Essa observação pode ser generalizada, como veremos a seguir, para um grupo arbitrário $(G, *)$ e para um subgrupo arbitrário $H$ de $G$. Para a demonstração desse fato usaremos mais uma vez, por simplicidade, a notação multiplicativa para indicar a operação do grupo $G$.

**Proposição 19:** (i) A relação $\approx$ sobre $G$ definida por "$a \approx b$ se, e somente se, $a^{-1}b \in H$" é uma relação de equivalência. (ii) Se $a \in G$, então a classe de equivalência determinada por $a$ é o conjunto $aH = \{ah \mid h \in H\}$.

*Demonstração:*

(i)

• Como $e = a^{-1}a \in H$, então $a \approx a$ e, portanto, vale a reflexividade para a relação em estudo.

• Se $a \approx b$, então $a^{-1}b \in H$; mas, sendo $H$ um subgrupo de $G$, então $(a^{-1}b)^{-1} = b^{-1}a \in H$. Isso mostra que $b \approx a$ e, portanto, que a simetria também se verifica para $\approx$.

• Suponhamos $a \approx b$ e $b \approx c$; então $a^{-1}b, b^{-1}c \in H$; daí, $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$ e, portanto, $a \approx c$, de onde a transitividade também vale neste caso.

(ii)

• Seja $\bar{a}$ a classe de equivalência do elemento $a$. Se $x \in \bar{a}$, então $x \approx a$, ou seja, $x^{-1}a \in H$. Portanto, $x^{-1}a = h$, para um conveniente elemento $h \in H$. Daí, $x = ah^{-1}$ e, portanto, $x \in aH$, uma vez que $h^{-1} \in H$.

• Por outro lado, se $x \in aH$, então $x = ah$, para algum $h \in H$. Daí, $x^{-1}a = h^{-1} \in H$ e, portanto, $x \approx a$. De onde, $x \in \bar{a}$.

Dessas conclusões, segue que $\bar{a} = aH$. #

**Definição 10:** Para cada $a \in G$, a classe de equivalência $aH$ definida pela relação $\approx$ introduzida na proposição 19 é chamada *classe lateral à direita, módulo* H, determinada por $a$.

Uma decorrência imediata da proposição anterior é que o conjunto das classes laterais à direita, módulo $H$, determina uma partição em $G$, ou seja:

a) se $a \in G$, então $aH \neq \emptyset$;

b) se $a, b \in G$, então $aH = bH$ ou $aH \cap bH = \emptyset$;

c) a união de todas as classes laterais é igual a $G$.

O conjunto quociente de G por essa relação, denotado por $G/H$, é o conjunto das classes laterais $aH (a \in G)$. Um dos elementos desse conjunto é o próprio $H$, pois $H = eH$

De maneira análoga se demonstra que a relação $\sim$ definida por "$a \sim b$ se, e somente se, $ab^{-1} \in H$" também é uma relação de equivalência sobre o grupo $G$. Só que, neste caso, a classe de equivalência de um elemento $a \in G$ é o subconjunto $Ha = \{ha \mid h \in H\}$, chamado *classe lateral à esquerda, módulo* H, *determinada por a*. É claro que, se $G$ for comutativo, então $aH = Ha$, para qualquer $a \in G$.

Na teoria que segue é indiferente usar classes laterais à esquerda (com as quais trabalharemos) ou à direita. Um dos motivos é que os conjuntos quocientes têm a mesma cardinalidade nos dois casos. De fato, pode-se demonstrar que a correspondência $aH \to Ha^{-1}$ é uma bijeção (propomos esse resultado como exercício)

*Exemplo 32:* No grupo multiplicativo $G = \{1, -1, i, -i\}$ das raízes quárticas da unidade, consideremos o subgrupo $H = \{1, -1\}$. As classes laterais neste caso são:

$$1H = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\}$$
$$(-1)H = \{(-1) \cdot 1, (-1) \cdot (-1)\} = \{-1, 1\}$$
$$iH = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\}$$
$$(-i)H = \{(-i) \cdot 1, (-i)(-1)\} = \{-i, i\}$$

Portanto, $G/H = \{1H, iH\}$.

Nesta altura convém registrar que, se $H$ é um subgrupo de um grupo aditivo $G$, então as classes laterais à direita, módulo $H$, são os conjuntos $a + H$, com $a \in G$.

*Exemplo 33:* Seja $G$ o grupo aditivo $\mathbb{Z}_6$. Para facilitar, escreveremos os elementos de $\mathbb{Z}_6$ sem os traços. Ou seja, $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Considerando o subgrupo $H = \{0, 3\}$, temos:

$$0 + H = H = \{0, 3\}, \quad 1 + H = \{1, 4\} \quad \text{e} \quad 2 + H = \{2, 5\}$$

Como a reunião dessas 3 classes é igual a $G$, podemos interromper nossos cálculos nesta altura, com a certeza de que não há mais classes distintas das que já foram obtidas. Portanto, $G/H = \{H, 1 + H, 2 + H\}$.

*Exemplo 34:* Considere o grupo multiplicativo $\mathbb{R}^*$ dos números reais e $H$ o subgrupo formado pelos números reais estritamente positivos. Ou seja, $H = \{x \in \mathbb{R}^* \mid x > 0\}$. Como

$$aH = H, \text{ se } a > 0$$
$$aH = \{x \in \mathbb{R}^* \mid x < 0\}, \text{ se } a < 0$$

então $\mathbb{R}^*/H$ é formado de duas classes apenas: a dos números reais maiores que zero e a dos números reais menores que zero.

*Exemplo 35:* Consideremos agora o grupo simétrico $G = S_3$. Para facilitar, adotemos a notação

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Isso posto, $S_3 = \{e, a, a^2, b, ba, ba^2\}$ (ver **2.4**, xii b). Considerando-se o subgrupo $H = C_3 = \{e, a, a^2\}$, então:

$$eH = H = \{e, a, a^2\}$$
$$aH = \{ae, aa, aa^2\} = \{a, a^2, e\}$$
$$a^2H = \{a^2e, a^2a, a^2a^2\} = \{a^2, e, a\}$$
$$bH = \{b, ba, ba^2\}$$

Também aqui já não é preciso prosseguir (mesma explicação do exemplo 33). Portanto, $S_3/C_3 = \{H, bH\}$.

**Proposição 20:** Seja $H$ um subgrupo de $G$. Então duas classes laterais quaisquer módulo $H$ são subconjuntos de $G$ que têm a mesma cardinalidade.

*Demonstração:* Dadas duas classes laterais $aH$ e $bH$, temos de mostrar que é possível construir uma aplicação bijetora $f: aH \to bH$. Lembrando a forma geral dos elementos dessas classes, é natural definir $f$ da seguinte maneira: $f(ah) = bh$, para qualquer $h \in H$. Sem maiores dificuldades, prova-se que $f$ é injetora e sobrejetora. De fato:

• (injetora) Se $h, h_1 \in H$ e $f(ah) = f(ah_1)$, então $bh = bh_1$; como, porém, todo elemento de $G$ é regular, então $h = h_1$.

• (sobrejetora) Seja $y \in bH$. Então $y = bh$, para algum $h \in bH$. Tomando-se $x = ah \in aH$, então $f(x) = f(ah) = bh = y$. #

Em particular, todas as classes têm a mesma cardinalidade de $H = eH$ ($e$ = *elemento neutro*).

Obviamente, se $G$ é um grupo finito, então o conjunto $G/H$ também é finito. O número de elementos distintos de $G/H$ é chamado *índice de H em G* e é denotado por $(G : H)$. Então, no exemplo 32, $(G : H) = 2$, no exemplo 33, $(G : H) = 3$, no exemplo 34, $(G : H) = 2$ e no exemplo 35, $(G : H) = 2$.

Devido ao fato de que $aH \to Ha^{-1}$ é uma aplicação bijetora, como já observamos, então o índice de $H$ em $G$ é o mesmo, quer se considerem classes laterais à direita ou à esquerda, módulo $H$.

## 14. O TEOREMA DE LAGRANGE

**Proposição 21** (teorema de Lagrange): Seja $H$ um subgrupo de um grupo finito $G$. Então $o(G) = o(H)(G : H)$ e, portanto, $o(H) \mid o(G)$.

*Demonstração:* Suponhamos $(G : H) = r$ e seja $G/H = \{a_1H, a_2H, ..., a_rH\}$. Então, devido à proposição 19, $G = a_1H \cup a_2H \cup ... \cup a_rH$ e $a_iH \cap a_jH = \emptyset$, sempre que $i \neq j$. Mas, devido à proposição 20, o número de elementos de cada uma das classes laterais é igual ao número de elementos de $H$, ou seja, é igual a $o(H)$. Portanto:

$$o(G) = o(H) + o(H) + ... + o(H)$$

em que o numero de parcelas é $r = (G : H)$. De onde:

$$o(G) = (G : H)o(H)$$

e $o(H) \mid o(G)$. #

Diga-se de passagem que, apesar do nome, não é de Lagrange, matemático do qual já falamos na abertura deste capítulo, a demonstração geral que acabamos de fazer desse teorema. Na época de Lagrange, o conceito geral de grupo ainda não havia sido formulado. Na verdade, Lagrange apenas usou o teorema numa situação

muito particular mas extremamente importante, em pesquisa que visava encontrar uma ligação entre a solução algébrica das equações e as permutações das raízes dessas equações

**Corolário 1:** Seja $G$ um grupo finito. Então a ordem (período) de um elemento $a \in G$ divide a ordem de $G$ e o quociente é $(G : H)$, em que $H$ [illegible] $[a]$

*Demonstração:* Basta lembrar que a ordem de $a$ é igual à ordem de $[a]$ e que, devido ao teorema de Lagrange.

$$o(G) = (G : H)o([a]). \#$$

**Corolário 2:** Se $a$ é um elemento de um grupo finito $G$, então $a^{o(G)} = e$ (elemento neutro do grupo).

*Demonstração:* Seja $h$ a ordem de $a$. Portanto, $h$ é o menor inteiro estritamente positivo tal que $a^h = e$ (elemento neutro do grupo). Mas, devido ao corolário anterior:

$$o(G) = (G : H)h$$

em que $H = [a]$. Portanto:

$$a^{o(G)} = a^{(G : H)h} = (a^h)^{(G : H)} = e^{(G : H)} = e. \#$$

**Corolário 3:** Seja $G$ um grupo finito cuja ordem é um número primo. Então $G$ é cíclico e os únicos subgrupos de $G$ são os triviais, ou seja, $\{e\}$ e o próprio $G$.

*Demonstração:* Seja $p = o(G)$. Como $p > 1$, o grupo $G$ possui um elemento $a$ diferente do elemento neutro. Assim, se $H = [a]$, o teorema de Lagrange garante que $o(H) \mid p$. Logo, $o(H) = 1$ ou $p$ e, portanto, $H = \{e\}$ ou $H = G$. Como a primeira dessas hipóteses é impossível, então $G = H$ e, portanto, $G$ é cíclico. Por outro lado, se $J$ é um subgrupo de $G$, então, ainda devido ao teorema de Lagrange, $o(J) \mid o(G)$. Daí, $o(J) = 1$ ou $p$ e, portanto, $J = \{e\}$ ou $J = G$. #

*Contra-exemplo 2:* Considere o seguinte subconjunto do grupo $S_4$: $L = \left\{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}\right\}$. Embora o número de elementos de $L$, que é 2, divida a ordem do grupo $S_4$, que é 24, $L$ não é um subrupo de $S_4$, uma vez que $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \notin L$. Isso mostra que não vale a recíproca do teorema de Lagrange.

*Exemplo 36:* O teorema de Lagrange pode ajudar bastante na determinação dos subgrupos de um grupo finito. Para exemplificar, consideremos o grupo $S_3$, cuja ordem é 6, como já vimos. Os subgrupos possíveis de $S_3$ têm, portanto, ordem 1, 2, 3 ou 6. Os de ordem 1 e 6 são triviais: respectivamente, o subgrupo formado só pelo elemento neutro e o próprio $S_3$. Os de ordem 2 e 3 são necessariamente cíclicos, como vimos (corolário 3). Logo (ver exemplo 25), $S_3$ tem três subgrupos de ordem 2, a saber, $[g_1]$, $[g_2]$ e $[g_3]$ e um único de ordem três: $[f_1]$ [illegible] $[f_2]$

É claro que o exemplo dado é muito favorável na aplicação do teorema de Lagrange. No caso do grupo $S_4$, o teorema de Lagrange também é suficiente, embora o trabalho seja muito maior. Vale ressaltar, porém, que há outros recursos teóricos capazes de favorecer uma pesquisa mais abrangente dos subgrupos de um grupo finito, mas eles se situam além dos objetivos deste livro.

### Exercícios

**99.** Determine todas as classes laterais de $H - \{\bar{0}, 3, 6, 9\}$ no grupo aditivo $\mathbb{Z}_{12}$.

**100.** Determine todas as classes laterais de $4\mathbb{Z}$ no grupo aditivo $\mathbb{Z}$.

**101.** Seja $S_3$ o grupo das permutações de $E = \{1, 2, 3\}$. Determine todas as classes laterais de $H = \{f_0, f_1\}$ subgrupo de $S_3$ em que:

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{e} \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

**102.** Sendo $H = \{0, \pm m, +2m, \ldots\}$, $m \in \mathbb{Z}$, um subgrupo do grupo aditivo $\mathbb{Z}$, mostre que $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\} = \mathbb{Z}_m$ é o conjunto das classes laterais de $H$. (Logo, $(\mathbb{Z} : H) = m$.)

**103.** É finito ou infinito o número de classes de $\mathbb{Z} \times 2\mathbb{Z}$ em $\mathbb{Z} \times \mathbb{Z}$? Por quê?

**104.** Dado o grupo $\mathbb{Z} \times \mathbb{Z}_2$ (produto direto), ache todas as classes laterais, à esquerda, do subgrupo $H = \{0\} \times \mathbb{Z}_2$.

**105.** Mostre que o número de classes laterais de $\mathbb{R}$ em $\mathbb{C}$ é infinito.

**106.** Considerando $\mathbb{Z}$ como subgrupo do grupo aditivo $\mathbb{Q}$, descreva as classes $\mathbb{Z} + (-1)$ e $\mathbb{Z} + \frac{1}{2}$.

**107.** Mostre que, sendo $a + \mathbb{Z}$ uma classe lateral de $\mathbb{Z}$ em $\mathbb{R}$ ($a \in \mathbb{R}$), então existe $b \in \mathbb{R}$ tal que $0 \leqslant b < 1$ e $b + \mathbb{Z} = a + \mathbb{Z}$.

**108.** Mostre que, dado $a (a \in \mathbb{C}^*)$, então existe $b \in \mathbb{C}^*$ tal que $|b| \quad 1$ e $b\,\mathbb{R}^*_+ \quad a\,\mathbb{R}^*$.

**109.** a) Mostre que $H \quad \left\{\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \mid c \in \mathbb{R}^*\right\}$ é um subgrupo do grupo $GL_2(\mathbb{R})$.

b) Mostre que existem infinitas classes de $H$ em $G$.

**110.** Mostre que são equipotentes os conjuntos das classes laterais à esquerda e o das classes laterais à direita para todo subgrupo de um grupo $G$, ou seja, têm o mesmo cardinal.
*Sugestão:* Considerar $\varphi(aH) = Ha^{-1}$.

**111.** Seja $H$ um subgrupo de um grupo $(G, \cdot)$
a) Mostre que "$x \sim y \Leftrightarrow x^{-1}y \in H$" define uma relação de equivalência em $G$.
b) Mostre que, $\forall a \in G, \bar{a} = aH$.

**112.** Seja $G$ um grupo de ordem $p^n$, em que $p$ é primo e $n > 1$. Mostre que a ordem de um elemento qualquer de $G$ é uma potência de $p$.

**113.** Seja $f: G \to J$ um homomorfismo de grupos. Sendo $S$ um subgrupo de $J$, prove que $f^{-1}(S)$ é subgrupo de $G$ tal que $N(f) \subset f^{-1}(S)$.

**Exercícios complementares**

**C5.** Sejam $H$ e $K$ subgrupos de um grupo finito. Se $o(H) = p$ e $o(K) = q$ ($p \neq q$ primos), então $H \cap K = \{e\}$. Prove.

**C6.** Demonstre que todo subgrupo próprio do grupo aditivo dos números racionais tem índice infinito.

# IV-5 SUBGRUPOS NORMAIS — GRUPOS QUOCIENTES

## 15. INTRODUÇÃO

Como já vimos na nota histórica que abre este capítulo, a noção de grupo e a própria palavra "grupo", ainda que com um significado não muito claro, ocorreram primeiramente ao matemático Evariste Galois. A questão que levou Galois a essa noção era a da resolubilidade das equações por meios algébricos (por radicais). Galois associou a cada equação um grupo de permutações de suas raízes e conseguiu vincular a resolubilidade a uma propriedade desse grupo. Os grupos com essa propriedade são chamados modernamente de *grupos solúveis*.

Ocorre que o conceito de grupo solúvel envolve um conceito preliminar, o de *subgrupo normal*, que Galois também teve de criar. De fato, na linguagem algébrica moderna, um grupo $G$ se diz *solúvel* se é possível encontrar uma sucessão finita de subgrupos $G_0, G_1, G_2, ..., G_n$ tais que: (i) $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_n = \{e\}$ ($e$ = elemento neutro de $G$); (ii) $G_{i+1}$ é "subgrupo normal" de $G_i$ ($i = 0, 1, ..., n - 1$), (iii) o "grupo quociente" $G_i/G_{i+1}$ é abeliano.

Pois bem, são justamente os conceitos de "subgrupo normal" e "grupo quociente" que introduziremos nesta seção. Deixamos claro, porém, que o conceito de grupo solúvel e seus desdobramentos na teoria das equações não serão explorados aqui, devido ao caráter introdutório deste trabalho.

Também nesta seção, e pelas mesmas razões de sempre, adotaremos a notação multiplicativa para as operações dos grupos no desenvolvimento da teoria.

## 16. MULTIPLICAÇÃO DE SUBCONJUNTOS

Sejam $(G, \cdot)$ um grupo e $A$ e $B$ subconjuntos de $G$. Indicaremos por $AB$ e chamaremos de *produto* de $A$ por $B$ o seguinte subconjunto de $G$:

$$AB = \varnothing, \text{ se } A = \varnothing \text{ ou } B = \varnothing$$

$$AB = \{xy \mid x \in A \text{ e } y \in B\}, \text{ se } A \neq \varnothing \text{ e } B \neq \varnothing$$

Portanto, a "lei" que associa a cada par $(A, B)$ de subconjuntos de $G$ seu produto $AB$ é uma operação sobre o conjunto $\mathcal{P}(G)$ das partes de $G$, chamada *multiplicação de subconjuntos* de $G$. Essa operação goza da propriedade associativa (pelo fato de a multiplicação de $G$ gozar dessa propriedade). Vale notar, ainda, que, se o grupo $G$ é comutativo, então a multiplicação de subconjuntos de $G$ goza da propriedade comutativa.

*Exemplo 37:* Seja $G = \{e, a, b, c\}$ um grupo de Klein. Lembremos a tábua desse grupo.

| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

Se $A = \{e, a\}$ e $B = \{b, c\}$, então $AB = \{eb, ec, ab, ac\} = \{b, c, c, b\} = \{b, c\}$.

*Exemplo 38:* Consideremos o grupo multiplicativo dos números reais. Se

$$A = \{x \in \mathbb{R}^* \mid x > 0\} \text{ e } B = \{x \in \mathbb{R}^* \mid x < 0\}$$

então:

$$AB = \{x \in \mathbb{R}^* \mid x < 0\} = B$$

pois o produto de um número estritamente positivo por um estritamente negativo é estritamente negativo e, por outro lado, todo número estritamente negativo $a$ pode ser escrito como $a = (-1)(-a)$, em que o primeiro fator é estritamente negativo e o segundo estritamente positivo.

## 17. SUBGRUPOS NORMAIS

**Definição 11:** Um subgrupo $N$ de um grupo $G$ é chamado *subgrupo normal* (ou *invariante*) se, para todo $x \in G$, se verifica a igualdade

$$xN = Nx.$$

Ou seja, a classe lateral à direita, módulo $N$, determinada por $x$, é igual à classe lateral à esquerda, módulo $N$, determinada por $x$, para qualquer $x \in G$

*Exemplo 39:* Se $G$ é abeliano, então obviamente todo subgrupo de $G$ é normal.

*Exemplo 40:* Consideremos o grupo simétrico $S_3$. Lembremos que, se $f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, então $S_3 = \{f_0, f_1, f_1^2, g_1, g_1f_1, g_1f_1^2\}$.

Embora esse grupo não seja comutativo, o subgrupo $H = C_3 = \{f_0, f_1, f_1^2\}$ é normal, pois, como se pode ver, conferindo em sua tábua (ver **2.4** xii.b):

$f_0H = \{f_0, f_1, f_1^2\} = Hf_0$ $\qquad g_1H = \{g_1, g_1f_1, g_1f_1^2\} = Hg_1$

$f_1H = \{f_1, f_1^2, f_0\} = Hf_1$ $\qquad (g_1f_1)H = \{g_1f_1, g_1f_1^2, g_1\} = H(g_1f_1)$

$f_1^2H = \{f_1^2, f_0, f_1\} = Hf_1^2$ $\qquad (g_1f_1^2)H = \{g_1f_1^2, g_1, g_1f_1\} = H(g_1f_1^2)$

Portanto, só há duas classes laterais distintas: $f_0H$ e $g_1H$. Sugerimos ao leitor verificar os "cálculos" na tábua.

*Exemplo 41:* Seja $H$ um subgrupo de $G$ tal que $(G : H) = 2$. Então $H$ é um subgrupo normal de $G$. De fato, neste caso, as classes laterais à direita, módulo $H$, são duas: $H$ e $aH$, em que $a$ é um elemento qualquer do grupo que nao pertence a $H$, e, portanto, $aH$ $(H^c)_G$, pois as duas classes formam uma partição de $G$ As classes laterais à esquerda, módulo $H$, também são duas. $H$ e $Ha$, em que $a$ é um elemento qualquer do grupo que não pertence a $H$, e, portanto, $Ha$ $(H^c)_G$. Logo, $xH - Hx$, qualquer que seja $x \in G$.

**Proposição 22:** Seja $N$ um subgrupo normal do grupo $G$. Entao, para quaisquer $a, b \in G$, vale a igualdade $(aN)(bN) - (ab)N$.

*Demonstração:* A demonstração será feita por dupla inclusão.

• Seja $x \in (aN)(bN)$. Então, devido à definição de produto de subconjuntos, $x = uv$, em que $u \in aN$ e $v \in bN$. Portanto, $u = an_1$ e $v = bn_2$, para convenientes $n_1, n_2 \in N$; daí, $x = (an_1)(bn_2) = a(n_1b)n_2$. Como, porém, por hipótese, $Nb = bN$ e $n_1b \in Nb$, então $n_1b = bn_3$, para algum $n_3 \in N$. De onde, $x = a(n_1b)n_2 = a(bn_3)n_2 = (ab)(n_3n_2)$. Observando-se que $n_3n_2 \in N$, conclui-se que $x \in (ab)N$. Fica provado, pois, que $(aN)(bN) \subset (ab)N$.

• Seja $x \in (ab)N$. Então, $x = (ab)n$, para algum $n \in N$. Mas nessa igualdade é possível introduzir o elemento neutro $e$ da seguinte maneira: $x = (ae)(bn)$. Como $e \in N$, então $ae \in aN$. Por outro lado, é imediato que $bn \in bN$. De onde, $x = (ab)n = (ae)(bn) \in$ $\in (aN)(bN)$. Ficou demonstrado, assim, que $(ab)N \subset (aN)(bN)$.

Das conclusões parciais, segue a tese: $(ab)N = (aN)(bN)$. #

A proposição anterior nos diz, basicamente, que o conjunto das classes laterais à direita, módulo $N$, que é uma parte de $\mathcal{P}(G)$ denotada por $G/N$, é fechado em relação à multiplicação de subconjuntos de $G$ A associatividade da multiplicação de

classes laterais é uma conseqüência desse fechamento e da associatividade da multiplicação de subconjuntos, mas poderia ser demonstrada diretamente assim:

$[(aN)(bN)](cN) = [(ab)N](cN) = [(ab)c]N = [a(bc)]N = (aN)[(bc)N] = (aN)[(bN)(cN)]$

## 18. GRUPOS QUOCIENTES

Seja $N$ um subgrupo normal de $G$. As seguintes propriedades, envolvendo a multiplicação de subconjuntos de $G$, restrita a $G/N$, já foram destacadas nesta seção:

- $(aN)(bN) = (ab)N$;
- $[(aN)(bN)](cN) = (aN)[(bN)(cN)]$.

Além dessas, valem também:

- $(aN)(eN) = (ae)N = aN = (ea)N = (eN)(aN)$;
- $(aN)(a^{-1}N) = (aa^{-1})N = eN = (a^{-1}a)N = (a^{-1}N)(aN)$.

Portanto, o conjunto quociente $G/N$, com a multiplicação de subconjuntos, restrita a seus elementos, é um grupo cujo elemento neutro é $eN = N$ e no qual $(aN)^{-1} = a^{-1}N$.

**Definição 12:** Sejam $G$ um grupo e $N$ um subgrupo normal de $G$. Nessas condições, o *grupo quociente de G por N* é o par formado pelo conjunto quociente $G/N$ e a restrição aos elementos desse conjunto da multiplicação de subconjuntos de $G$.

*Exemplo 42:* Sejam $G = \{1, -1, i, -i\}$ o grupo multiplicativo das raízes quárticas da unidade e $N = \{1, -1\}$. $N$ é um subgrupo normal de $G$ pelo fato mesmo de que $G$ é comutativo. As classes laterais neste caso são duas apenas. $1N = N = \{1, -1\}$ e $iN = \{i, -i\}$ (O próprio fato de a união das duas ser igual a $G$ é suficiente para mostrar que não há outras.) A tábua do grupo quociente $G/N$ é.

| $\cdot$ | $N$ | $iN$ |
|---|---|---|
| $N$ | $N$ | $iN$ |
| $iN$ | $iN$ | $N$ |

*Exemplo 43:* Sejam $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ e $H = \{0, 3\}$. As classes laterais neste caso são: $0 + H = H$, $1 + H = \{1, 4\}$, $2 + H = \{2, 5\}$, já que essas três englobam todos os elementos de $\mathbb{Z}_6$. A tábua do grupo quociente $G/H$ neste caso é:

| $+$ | $H$ | $1 + H$ | $2 + H$ |
|---|---|---|---|
| $H$ | $H$ | $1 + H$ | $2 + H$ |
| $1 + H$ | $1 + H$ | $2 + H$ | $H$ |
| $2 + H$ | $2 + H$ | $H$ | $1 + H$ |

Notar que usamos o fato de que $3 + H = H$, pois $3 - 0 = 3 \in H$.

*Exemplo 44:* No grupo $S_3$ consideremos o subgrupo $H = C_3 = \{f_0, f_1, f_1^2\}$ No exemplo 40 verificou-se que $H$ é um subgrupo normal $S_3$. Outra maneira de chegar a essa conclusão seria por intermédio do exemplo 41. A tábua do grupo quociente $S_3/H$ é a seguinte:

| $\circ$ | $H$ | $g_1H$ |
|---|---|---|
| $H$ | $H$ | $g_1H$ |
| $g_1H$ | $g_1H$ | $H$ |

**Proposição 23:** Seja $f: G \to L$ um homomorfismo de grupos. Se $N$ é um subgrupo normal de $G$, então a aplicação $\mu: G \to G/N$ definida por $\mu(a) = aN$ é um homomorfismo sobrejetor de grupos cujo núcleo é $N$.

*Demonstração:* De fato:

- $\mu(ab) = (ab)N = (aN)(bN) = \mu(a)\mu(b)$.

- Se $y \in G/N$, então $y = aN$, para algum $a \in G$. Como, então, $\mu(a) = aN = y$, conclui se que $\mu$ é uma aplicação sobrejetora.

- Lembremos, primeiro, que o elemento neutro do grupo quociente é a classe $N$. Isso posto se $a \in Ker(\mu)$, então $\mu(a) = aN = N$. Como, porém, $a \in aN$, pois $a = ae$ e $e \in N$, então $a \in N$. Isso mostra que $Ker(\mu) \subset N$. Por outro lado, se $a \in N$, então $aN = N$ e, portanto, $\mu(a) = aN = N$ (elemento neutro de $G/N$) e, portanto, $a \in Ker(\mu)$. As duas inclusões demonstradas garantem que $Ker(\mu) = N$. #

**Definição 13:** Seja $f: G \to L$ um homomorfismo de grupos Se $N$ é um subgrupo normal de $G$, então o homomorfismo $\mu: G \to G/N$ definido por $\mu(a) = aN$ é chamado *homomorfismo canônico* de $G$ sobre $G/N$.

## 19. O TEOREMA DO HOMOMORFISMO

**Lema 1:** Se $f: G \to L$ é um homomorfismo de grupos, então $N = Ker(f)$ é um subgrupo normal de $G$ e, portanto, $G/N$ tem uma estrutura de grupo.

*Demonstração:* Que $N = Ker(f)$ é um subgrupo de $G$ já foi demonstrado (proposição 6). Falta provar que é normal, ou seja, que $aN = Na$, para qualquer $a \in G$, o que será feito por dupla inclusão.

- Se $x \in aN$, então $x = ah$, para algum $h \in N$. Mas $ah = (aha^{-1})a$. Ocorre, porém, que $f(aha^{-1}) = f(a)f(h)f(a^{-1}) = f(a)e[f(a)]^{-1} = f(a)[f(a)]^{-1} = u$ (elemento neutro de $L$). Portanto, $aha^{-1} \in N = Ker(f)$ e, como $x = ah = (aha^{-1})a$, então $x \in Na$. Fica provado, pois, que $aN \subset Na$.

- De maneira análoga se demonstra que $Na \subset aN$.

Das duas conclusões, segue que $Na = aN$, como queríamos provar #

**Proposição 24** (teorema do homomorfismo para grupos) Seja $f: G \to L$ um homomorfismo sobrejetor de grupos. Se $N = Ker(f)$, então o grupo quociente $G/N$ é isomorfo ao grupo $L$.

*Demonstração:* O primeiro passo é descobrir um isomorfismo, digamos, de $G/N$ em $L$. E, para isso, uma boa pista é ver como se representam os elementos de $G/N$ e $L$. Os do grupo quociente são classes laterais $aN$, com $a \in G$, e os de $L$ imagens $f(a)$, com $a \in G$. Portanto, é natural investigar se a correspondência $aN \to f(a)$ é um isomorfismo. Mas primeiro é preciso ver se se trata de uma aplicação, já que uma mesma classe lateral à direita, módulo $N$, pode ser representada em geral de mais de uma maneira.

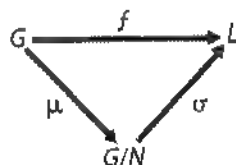
• Vamos supor $aN = bN$. Então $b^{-1}a \in N$ e, portanto, $f(b^{-1}a) = u$ (elemento neutro de $L$). Mas $f(b^{-1}a) = f(b^{-1})f(a) = [f(b)]^{-1}f(a)$. Logo, $[f(b)]^{-1}f(a) = u$ e $f(a) = f(b)u = f(b)$. De onde, a correspondência $aN \to f(a)$ é de fato uma aplicação.

• Seja $\sigma: G/N \to L$ a aplicação definida por $\sigma(aN) = f(a)$. Para mostrar que $\sigma$ é injetora, suponhamos $f(a) = f(b)$, em que $a, b \in G$. Então $[f(b)]^{-1}f(a) = [f(b)]^{-1}f(b) = u$. Usando-se a hipótese de que $f$ é um homomorfismo de grupos, da igualdade $[f(b)]^{-1}f(a) = u$ segue que $f(b^{-1}a) = u$. Mas isso significa que $b^{-1}a \in N$ e, portanto, $aN = bN$, como queríamos provar.

• Que $\sigma$ é sobrejetora é praticamente imediato. De fato, se $y \in L$, então $y = f(a)$, com $a \in G$. Então, tomando $x = aN \in G/N$, $\sigma(x) = \sigma(aN) = f(a) = y$.

• Mostremos por último que $\sigma$ é um homomorfismo de grupos. De fato:

$$\sigma[(aN)(bN)] = \sigma[(ab)N] = f(ab) = f(a)f(b). \#$$

Seja $f: G \to L$ um homomorfismo sobrejetor de grupos e denotemos por $N$ o núcleo de $f$. Consideremos ainda o grupo quociente $G/N$, o homomorfismo canônico $\mu: G \to G/N$ e o homomorfismo $\sigma: G/N \to L$, introduzido na proposição anterior. O diagrama de grupos e homomorfismos

sugere a possibilidade de uma fatoração de $f$ através de $G/N$. Efetivamente isso ocorre pois, para qualquer $a \in G$:

$$(\sigma \circ \mu)(a) = \sigma(\mu(a)) = \sigma(aN) = f(a)$$

e, portanto:

$$f = \sigma \circ \mu$$

*Exemplo 45:* Dado um inteiro $m > 1$, consideremos o homomorfismo $p_m: \mathbb{Z} \to \mathbb{Z}_m$ definido por $p_m(a) = \bar{a}$ (exemplo 11). Esse homomorfismo é sobrejetor, como já vimos, e seu núcleo é o conjunto dos inteiros $a$ tais que $\bar{a} = 0$, ou seja, o conjunto dos

inteiros $a$ tais que $a \equiv 0 \pmod{m}$. Portanto, $Ker(f) = [m] = \{0, \pm m, \pm 2m, ...\}$. O teorema do homomorfismo nos garante que os grupos $\mathbb{Z}/[m]$ e $\mathbb{Z}_m$ são isomorfos.

## Exercícios

**114.** Seja $G$ um grupo multiplicativo. Se $A \subset G$ e $A \neq \emptyset$, seja $A^{-1} = \{x^{-1} \mid x \in A\}$. Mostre que:

a) $(A^{-1})^{-1} = A$

b) $\forall A, B \subset G, A \neq \emptyset, B \neq \emptyset$, tem-se $(AB)^{-1} = B^{-1} \cdot A^{-1}$

**115.** Seja $G$ um grupo multiplicativo e $H \neq \emptyset$ um subconjunto de $G$. Mostre que $H$ é subgrupo de $G$ se, e somente se, $H \cdot H \subset H$ e $H^{-1} \subset H$.

**116.** Mostre que, se $N$ é subgrupo normal de $G$, $a \in G$ e $n \in N$, então existe um elemento $n' \in N$ tal que $an = n'a$.

**117.** Sejam $M$ e $N$ subgrupos normais de $G$. Mostre que $M \cap N$ e $MN$ também o são.

**Resolução**

Façamos $M \cap N = H$ e $MN = K$.

Sugerimos ao estudante mostrar que $H$ e $K$ são subgrupos de $G$.

Provemos que $xH = Hx, \forall \in G$:

$$\left.\begin{array}{l} y \in xH \Rightarrow y = xh \\ \qquad\qquad h \in M \cap N \end{array}\right\} \Rightarrow y = m'x = n'x$$

E, então, $m' = n' = h'$, isto é, $y = h'x \in Hx$.

Analogamente, $y \in Hx \Rightarrow y \in xH$.

Provemos que $xK = Kx, \forall \in G$:

$y \in xK \Rightarrow y = xk = x(mn) = (xm)n = (m'x)n = m'(xn) = m'(n'x) = (m'n')x = k'x \Rightarrow y \in Kx$

E, analogamente, $y \in Kx \Rightarrow y \in xK$. ∎

**118.** Sejam $G$ um grupo, $N$ um subgrupo normal e $H$ um subgrupo de $G$. Mostre que $H \cap N$ é normal em $H$.

**119.** Mostre que um subgrupo $N$ do grupo $G$ é normal se, e somente se, $x^{-1}Nx \subset N$, para todo $x \in G$. (*Nota*: $x^{-1}Nx = \{x^{-1}nx \mid n \in N\}$.)

**120.** Sejam $G$ um grupo e $H$ um subgrupo. Seja $N_H$ o conjunto de todos os $x \in G$ tais que $xHx^{-1} \subset H$. Mostre que $N_H$ é um grupo que contém $H$ e que $H$ é normal em $N_H$.

**121.** Mostre que, se $M$ e $N$ são subgrupos normais do grupo $G$ e $M \cap N = \{e\}$, então $mn = nm$, para todos $m \in M$ e $n \in N$.

*Sugestão:* Prove que $(mn)(nm)^{-1} = e$. ($e$ = elemento neutro)

**122.** Seja $N$ um subgrupo de $G$ tal que $(G : N) = 2$. Mostre que $N$ é normal em $G$.

**123.** Demonstre que, se um grupo finito $G$ tem um único subgrupo $N$ de uma dada ordem, então $N$ é normal em $G$.

**124.** Seja $G$ um grupo multiplicativo. Mostre que $H = \{x \in G \mid xa = ax, \forall a \in G\}$ é um subgrupo normal de $G$.

**Resolução**

1º) Sendo $e$ o elemento neutro de $G$, temos $ea = ae, \forall a \in G$; portanto, $e \in H$ e $H \neq \varnothing$.

2º) Sejam $x, y \in H$. Então $x$ e $y$ comutam com qualquer elemento de $G$. Interessa particularmente observar que, se $a \in G$, então $xa = ax$ e $ya^{-1} = a^{-1}y$.

Provemos que $xy^{-1} \in H$:

$(xy^{-1})a = x(y^{-1}a) = x(a^{-1}y)^{-1} = x(ya^{-1})^{-1} = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$

3º) Provemos, finalmente, que $aH = Ha, \forall a \in G$:

$\alpha \in aH \Leftrightarrow \alpha = ah \Leftrightarrow \alpha = ha \Leftrightarrow \alpha \in Ha$

Então, $aH \subset Ha$ e $aH \supset Ha$. ∎

**125.** Sejam $G$ um grupo, $H$ um subgrupo de $G$ e $N$ um subgrupo normal de $G$. Mostre que $NH$ é um subgrupo de $G$ e $NH = HN$.

**126.** Seja $f: G \to J$ um homomorfismo sobrejetor de grupos. Se $H$ é um subgrupo normal de $G$, mostre que $f(H)$ é um subgrupo normal de $J$.

**127.** Seja $f: G \to G'$ um homomorfismo com núcleo $H$. Suponha que $G$ é finito. Mostre que ordem de $G$ = (ordem da imagem de $f$)(ordem de $H$).

**128.** Sabe-se que o conjunto dos automorfismos de $G$, denotado por Aut($G$), é um grupo para a composição de aplicações. Para cada $a \in G$, seja $F_a: G \to G$ dada por $F_a(x) = axa^{-1}$, $\forall x \in G$. Mostre que $I(G) = \{F_a \mid a \in G\}$ é um subgrupo normal de Aut($G$).

**129.** Seja $T$ um subgrupo cíclico e normal de $G$. Mostre que todo subgrupo de $T$ é subgrupo normal de $G$.

**130.** Seja $G = [a]$ um grupo cíclico de ordem 6. Sendo $H = [a^2]$, construa a tábua do grupo $G/H$.

**Resolução**

$H = [a^2] = \{e, a^2, a^4\}$

As classes laterais à esquerda de $H$ são:

$eH = H$ e $aH = \{a, a^3, a^5\}$

Notemos que $eH = a^2H = a^4H$ e $aH = a^3H = a^5H$.

Observemos também que $xH = Hx$, $\forall x \in G$, pois $G$ é abeliano.

Podemos, então, construir a tábua de $G/H$:

| $\cdot$ | $H$ | $aH$ |
|---|---|---|
| $H$ | $H$ | $aH$ |
| $aH$ | $aH$ | $H$ |

■

**131.** Determine todos os subgrupos não triviais do grupo aditivo $\mathbb{Z}_6$. Para cada subgrupo $H$ encontrado, construa a tábua do grupo quociente $\mathbb{Z}_6/H$

**132.** Construa as tábuas dos seguintes grupos quocientes:

a) $\mathbb{Z}_8/H$, em que $H = \{\bar{0}, \bar{4}\}$

b) $\mathbb{Z}/2\mathbb{Z}$

c) $(\mathbb{Z} \times \mathbb{Z})/(3\mathbb{Z} \times 2\mathbb{Z})$, em que $\mathbb{Z} \times \mathbb{Z}$ é o produto direto

**133.** Considere $\mathbb{Z}$ como um subgrupo do grupo aditivo $\mathbb{Q}$ dos números racionais. Mostre que, dado um elemento $\bar{x} \in \mathbb{Q}/\mathbb{Z}$, existe um inteiro $n \geqslant 1$ tal que $n\bar{x} = \mathbf{0}$.

**134.** Demonstre que, se $H$ é um subgrupo normal de $G$ e o índice de $H$ em $G$ é um número primo, então $G/H$ é cíclico.

# IV-6 PERMUTAÇÕES

## 20. CICLOS E NOTAÇÃO CÍCLICA

Entre os grupos importantes que relacionamos em **2.4**, merece ser estudado um pouco mais profundamente, pela sua importância em vários campos, o grupo $S_n$ das permutações sobre o conjunto $I_n = \{1, 2, ..., n\}$, $n \geqslant 2$. Na nota histórica que abre este capítulo (seção 1), já nos referimos ao papel dos grupos de permutações na história das equações algébricas. Outro assunto em que os grupos de permutações desempenham um papel chave é na teoria dos determinantes.

Para o estudo que segue, precisaremos introduzir um novo tipo de permutação e uma nova notação.

**Definição 14:** Sejam $a_1, a_2, ..., a_r \in I_n$ inteiros distintos. Se $\sigma \in S_n$ é uma permutação tal que $\sigma(a_1) = a_2, \sigma(a_2) = \sigma^2(a_1) = a_3, ..., \sigma(a_{r-1}) = \sigma^{r-1}(a_1) = a_r$ e $\sigma(a_r) = \sigma^r(a_1) = a_1$ e $\sigma(x) = x$, para todo $x \in I_n - \{a_1, a_2, ..., a_r\}$, então se diz que $\sigma$ é um *ciclo de comprimento* r e que $\{a_1, a_2, ..., a_r\}$ é o *conjunto suporte* de $\sigma$. Para designar a permutação assim definida, usaremos a notação $(a_1, a_2, ..., a_r)$. Se $r = 2$, então $\sigma$ é chamado de *transposição*.

*Exemplo 46:* Consideremos em $S_5$ a permutação

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

Como $\sigma(1) = 4$, $\sigma(4) = 2$ e $\sigma(2) = 1$, $\sigma(3) = 3$ e $\sigma(5) = 5$, então $\sigma$ é um ciclo de comprimento 3 cujo conjunto suporte é $\{1, 2, 4\}$. Portanto, podemos escrever:

$$\sigma = (1 \;\; 4 \;\; 2)$$

A notação cíclica merece um comentário. Primeiro, ela não indica em que grupo $S_n$ se está. Por exemplo, se escrevemos $\sigma = (1 \;\; 4 \;\; 2)$, simplesmente, pode se tratar tanto da permutação do exemplo 46 como de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$$

De que permutação se trata realmente é determinado pelo contexto. Outro aspecto dessa notação é que o mesmo ciclo pode ser descrito de mais de uma maneira, pois cada um dos elementos do suporte pode ocupar a primeira posição, desde que não se mude a seqüência em que eles aparecem. Em $S_5$, por exemplo:

$$(1 \;\; 4 \;\; 2) = (4 \;\; 2 \;\; 1) = (2 \;\; 1 \;\; 4)$$

Em qualquer dessas três notações, $1 \mapsto 4$, $4 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$, $5 \mapsto 5$ e, portanto, efetivamente elas indicam a mesma permutação de $S_5$.

**Proposição 25:** Se $\sigma = (a_1 a_2 \dots a_r) \in S_n$ é um ciclo de comprimento $r > 1$, então $o(\sigma) = r$ e, portanto, se $\varepsilon$ indicar a permutação idêntica de $S_n$, $[\sigma] = \{\varepsilon, \sigma, \sigma^2, \dots, \sigma^{r-1}\}$.

*Demonstração:* Da definição de ciclo decorre diretamente que $\sigma^{i-1}(a_1) = a_i$ $(i = 1, 2, \dots, r)$ e $\sigma^r(a_1) = a_1$. Então $\sigma^i \neq \varepsilon$ sempre que $1 \leq i < r$, e, portanto, $r \leq o(\sigma)$. Por outro lado, se $i$ é um índice tal que $1 \leq i \leq r$, então $\sigma^r(a_i) = \sigma^r(\sigma^{i-1}(a_1)) =$ $= \sigma^{i-1}(\sigma^r(a_1)) = \sigma^{i-1}(a_1) = a_i$. Considerando-se que $\sigma(x) = x$ sempre que $x \neq a_i$ $(i = 1, 2, \dots, r)$, então $\sigma^r = \varepsilon$ e, por conseguinte, $o(\sigma) \leq r$. De onde, $o(\sigma) = r$. #

Dois ciclos, como $(1 \;\; 2 \;\; 4)$ e $(3 \;\; 5)$, em $S_5$, cujos suportes são conjuntos disjuntos, são chamados *ciclos disjuntos*.

**Proposição 26:** Dois ciclos disjuntos comutam.

*Demonstração:* Sejam $\varphi$ e $\sigma$ ciclos de $S_n$ disjuntos, com suportes iguais respectivamente a $A$ e $B$. Se $x$ é um elemento de $I_n$, há três hipóteses possíveis:

• $x \in A$.

Então, $(\varphi \circ \sigma)(x) = \varphi(\sigma(x)) = \varphi(x)$, ao passo que $(\sigma \circ \varphi)(x) = \sigma(\varphi(x)) = \varphi(x)$. Portanto, $\varphi \circ \sigma$ e $\sigma \circ \varphi$ coincidem em $A$.

• $x \in B$ (raciocínio análogo).

• $x \notin A$ e $x \notin B$.

Neste caso, $(\varphi \circ \sigma)(x) = \varphi(\sigma(x)) = \varphi(x) = x$, ao passo que $(\sigma \circ \varphi)(x) = \sigma(\varphi(x)) = \varphi(x) = x$. Portanto, $\varphi \circ \sigma$ e $\sigma \circ \varphi$ também coincidem fora de $A$ e $B$. #

**Proposição 27:** Toda *permutação* $\sigma \in S_n$, exceção feita à permutação idêntica, pode ser escrita univocamente (salvo quanto à ordem dos fatores) como um produto de ciclos disjuntos.

*Demonstração:* Supondo, para facilitar, que $\sigma(1) \neq 1$, consideremos a seqüência de imagens de 1 pelas potências sucessivas de $\sigma$:

$$\sigma^0(1) = 1, \sigma(1), \sigma^2(1) = (\sigma \circ \sigma)(1), \sigma^3(1), \ldots$$

Como $I_n$ é finito, os elementos dessa seqüência não podem ser todos distintos. Isso nos permite fazer a seguinte escolha: seja $r$ o menor expoente estritamente positivo tal que $\sigma^0(1) = 1, \sigma(1), \sigma^2(1), \sigma^3(1), \ldots, \sigma^{r-1}(1)$ sejam distintos mas $\sigma^r(1) = \sigma^j(1)$, para algum inteiro $j$ tal que $0 \leqslant j < r$. Daí segue que $\sigma^{r-j}(1) = 1 = \sigma^0(1)$, o que só é possível, dada nossa escolha de $r$, se $j = 0$. Portanto, $\sigma^r(1) = 1$. Obtém-se assim o ciclo:

$$\sigma_1 = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{r-1}(1))$$

que coincide com a restrição de $\sigma$ a seu conjunto suporte.

Indiquemos por $a$ o menor inteiro de $I_n$ que não aparece no suporte de $\sigma_1$ e tal que $\sigma(a) \neq a$. (Se nenhum $a$ de $I_n$ cumprisse essa desigualdade, a demonstração já se encerraria.) Repetindo-se o argumento anterior com a seqüência

$$\sigma^0(a) = a, \sigma(a), \sigma^2(a) = (\sigma \circ \sigma)(a), \sigma^3(a), \ldots$$

chega-se a um ciclo $\sigma_2$, que também coincide com a restrição de $\sigma$ a seu conjunto suporte.

Mostremos que $\sigma_1$ e $\sigma_2$ são disjuntos. De fato, suponhamos que $b$ fosse um elemento comum aos suportes desses dois ciclos. Então $b = \sigma^t(1) = \sigma^s(a)$, com, digamos, $0 \leqslant s \leqslant t$. Daí, $\sigma^{t-s}(1) = a$, o que coloca $a$ no suporte de $\sigma_1$, contrariamente a nossa escolha.

Esse processo certamente termina num número finito $m$ de passos. E, como $\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_m$ tem sobre os elementos de $I_n$ o mesmo efeito que $\sigma$, então:

$$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_m. \#$$

*Exemplo 47:* Vamos decompor em ciclos disjuntos a seguinte permutação de $S_8$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 8 & 3 & 7 & 5 & 2 & 4 \end{pmatrix}$$

Como $\sigma(1) = 1$, vamos começar o processo descrito na demonstração com o elemento 2:

$$2, \sigma(2) = 6, \sigma^2(2) = \sigma(\sigma(2)) = \sigma(6) = 5, \sigma(5) = 7, \sigma(7) = 2$$

Portanto:

$$\sigma_1 = (2 \quad 6 \quad 5 \quad 7)$$

Repetindo-se o processo a partir do 3:

$$3, \sigma(3) = 8, \sigma(8) = 4, \sigma(4) = 3$$

Então:

$$\sigma_2 = (3 \quad 8 \quad 4)$$

Portanto:

$$\sigma = (2 \quad 6 \quad 5 \quad 7) \circ (3 \quad 8 \quad 4)$$

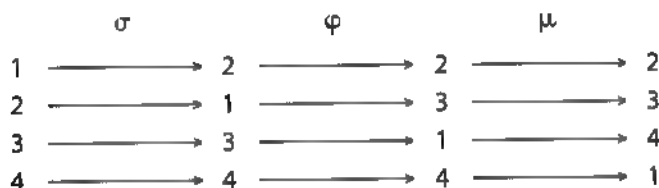
**Proposição 28:** Se $n > 1$, então toda permutação de $S_n$ pode ser expressa como um produto de transposições.

*Demonstração:* Uma verificação simples mostra que para todo ciclo de comprimento $r$ em $S_n$ vale a identidade

$$(a_1\ a_2\ a_3 \ldots a_{r-1}\ a_r) = (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \ldots \circ (a_1\ a_2)$$

Portanto, dada uma permutação de $S_n$, é só decompô-la em ciclos, de acordo com a proposição anterior, e depois aplicar a identidade acima para cada um dos ciclos. #

*Exemplo 48:* Justificar, com detalhes, a seguinte igualdade em $S_4$: $(1 \quad 2 \quad 3 \quad 4) = (1 \quad 4) \circ (1 \quad 3) \circ (1 \quad 2)$. Mostraremos que o efeito do produto de transposições do segundo membro sobre $I_4$ é igual ao do ciclo do primeiro membro. Para isso, façamos $(1 \quad 2) = \sigma$, $(1 \quad 3) = \varphi$ e $(1 \quad 4) = \mu$. Então:

$$\begin{array}{ccccccc}
 & \sigma & & \varphi & & \mu & \\
1 & \longrightarrow & 2 & \longrightarrow & 2 & \longrightarrow & 2 \\
2 & \longrightarrow & 1 & \longrightarrow & 3 & \longrightarrow & 3 \\
3 & \longrightarrow & 3 & \longrightarrow & 1 & \longrightarrow & 4 \\
4 & \longrightarrow & 4 & \longrightarrow & 4 & \longrightarrow & 1
\end{array}$$

o que mostra que $(\mu \circ \varphi \circ \sigma)(1) = 2$, $(\mu \circ \varphi \circ \sigma)(2) = 3$, $(\mu \circ \varphi \circ \sigma)(3) = 4$ e $(\mu \circ \varphi \circ \sigma)(4) = 1$ e, portanto, que $\mu \circ \varphi \circ \sigma = (1 \quad 2 \quad 3 \quad 4)$.

*Exemplo 49:* Vejamos como decompor em transposições a seguinte permutação de $S_8$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 8 & 3 & 7 & 5 & 2 & 4 \end{pmatrix}$$

Como já vimos (exemplo 47): $\sigma = (2 \quad 6 \quad 5 \quad 7) \circ (3 \quad 8 \quad 4)$. Mas, devido à identidade exibida no corolário:

$$(2 \quad 6 \quad 5 \quad 7) = (2 \quad 7) \circ (2 \quad 5) \circ (2 \quad 6) \quad \text{e} \quad (3 \quad 8 \quad 4) = (3 \quad 4) \circ (3 \quad 8)$$

Portanto:

$$\sigma = (2 \quad 7) \circ (2 \quad 5) \circ (2 \quad 6) \circ (3 \quad 4) \circ (3 \quad 8)$$

## 21. ASSINATURA DE UMA PERMUTAÇÃO

A decomposição de um ciclo em transposições, garantida pela proposição 28, não é única. De fato, como $(a \quad b) \circ (b \quad a)$ é a aplicação idêntica de $I_n$, que é o elemento neutro de $S_n$, então num produto de transposições podem-se inserir tantas expressões desse tipo quanto desejemos, sem afetar o resultado. Em $S_7$, por exemplo:

$(2 \quad 6 \quad 5 \quad 7) = (2 \quad 7) \circ (2 \quad 5) \circ (2 \quad 6) = (1 \quad 2) \circ (2 \quad 1) \circ (2 \quad 7) \circ (2 \quad 5) \circ (2 \quad 6)$

Pode-se demonstrar, porém, que todas as decomposições de um mesmo ciclo em transposições têm em comum a paridade. Ou seja, se numa delas o número de transposições é par (ímpar), então o mesmo acontece em todas as outras. Mas, para provar esse importante resultado, é preciso introduzir antes o conceito de *assinatura* de uma permutação.

**Definição 15:** A assinatura de uma permutação $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ é o número real, aqui denotado por $\operatorname{sgn} \sigma$, e definido por:

$$\operatorname{sgn} \sigma = \prod \frac{a_i - a_j}{b_i - b_j}$$

em que o produto é estendido a todos os pares $(i, j)$ de índices tais que $i > j$.

Da definição decorre diretamente que a assinatura da permutação idêntica é 1.

Convém observar que o produto que define $\operatorname{sgn} \sigma$ não depende da ordem das colunas na expressão de $\sigma$ e que cada quociente $\frac{a_i - a_j}{b_i - b_j}$ é uma função do par $(i, j)$.

*Exemplo 50:* A assinatura da *permutação*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

é:

$$\operatorname{sgn}(\sigma) = \frac{2-1}{3-2} \cdot \frac{3-1}{1-2} \cdot \frac{3-2}{1-3} = (1)(-2)(-1/2) = 1$$

**Proposição 29:** A assinatura de uma transposição é $-1$.

*Demonstração:* Seja $\tau \in S_n$ uma transposição.

Evidentemente podemos representar $\tau$ da seguinte maneira:

$$\tau = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_1 & a_3 & \dots & b_n \end{pmatrix}$$

Se $(r, s)$ é um par de índices da primeira linha da transposição $\tau$ e $1 \leq r < s \leq n$, então as situações possíveis são as seguintes:

a) $(r, s) = (1, 2)$ cujo fator correspondente em $\text{sgn}\,\tau$ é $\dfrac{a_2 - a_1}{a_1 - a_2} = -1$

b) $r = 1$ e $s > 2$, caso em que o fator correspondente de $(r, s)$ em $\text{sgn}\,\tau$ é $\dfrac{a_s - a_1}{a_s - a_2}$.

c) $r = 2$ e $s > 2$, caso em que o fator correspondente de $(r, s)$ em $\text{sgn}\,\tau$ é $\dfrac{a_s - a_2}{a_s - a_1}$.

d) $r > 2$ e, neste caso, o fator correspondente de $(r, s)$ em $\text{sgn}\,\tau$ é $\dfrac{a_s - a_r}{a_s - a_r} = 1$.

Como os fatores de b) e c) aparecem em pares cujo produto é 1, então:

$$\text{sgn}\,\tau = \frac{a_2 - a_1}{a_1 - a_2} = -1. \#$$

**Proposição 30:** Para quaisquer permutações $\sigma, \varphi \in S_n$, $\text{sgn}(\varphi \circ \sigma) = (\text{sgn}\,\varphi)(\text{sgn}\,\sigma)$.

*Demonstração:* Permutando convenientemente as colunas de $\varphi$, podemos escrever:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \quad \text{e} \quad \varphi = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

Portanto.

$$(\text{sgn}\,\varphi)(\text{sgn}\,\sigma) = (\text{sgn}\,\sigma)(\text{sgn}\,\varphi) = \prod \frac{a_i - a_j}{b_i - b_j} \prod \frac{b_i - b_j}{c_i - c_j} = \prod \frac{a_i - a_j}{c_i - c_j} = \text{sgn}\,(\varphi \circ \sigma). \#$$

**Corolário 1:** Se $\sigma \in S_n$, então $\text{sgn}\,\sigma = \pm 1$.

*Demonstração:* Como já vimos (proposição 28), toda permutação pode ser expressa como um produto de transposições. Portanto:

$$\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_r$$

para convenientes transposições $\tau_1, \tau_2, \dots, \tau_r \in S_n$. Então, usando-se a generalização natural da proposição 30 para $r$ fatores e considerando-se que a assinatura de uma transposição é igual a $-1$:

$$\begin{aligned} \text{sgn}\,\sigma &= \text{sgn}\,(\tau_1 \circ \tau_2 \circ \dots \circ \tau_r) = (\text{sgn}\ \tau_1)(\text{sgn}\ \tau_2) \dots (\text{sgn}\ \tau_r) = \\ &= (-1)(-1)\dots(-1) = (-1)^r = \pm 1. \# \end{aligned}$$

**Corolário 2:** Qualquer que seja a permutação $\sigma \in S_n$, $\text{sgn}\,\sigma^{-1} = (\text{sgn}\,\sigma)^{-1}$.

*Demonstração:* Como $(1\ \ 2) \circ (1\ \ 2)$ indica a identidade de $S_n$, então $\sigma^{-1} \circ \sigma = (1\ \ 2) \circ (1\ \ 2)$. Portanto:

$$\begin{aligned} [\text{sgn}\,(\sigma^{-1})](\text{sgn}\,\sigma) &= \text{sgn}\,(\sigma^{-1} \circ \sigma) = \text{sgn}\,[(1\ \ 2) \circ (1\ \ 2)] = \\ &= [\text{sgn}\,(1\ \ 2)][\text{sgn}\,(1\ \ 2)] = (-1)(-1) = 1 \end{aligned}$$

De onde, $\text{sgn}\,\sigma^{-1} = (\text{sgn}\,\sigma)^{-1}$. #

**Proposição 31:** Seja dada uma permutação $\sigma \in S_n$ e consideremos duas decomposições de $\sigma$ em transposições:

$$\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_r \quad \text{e} \quad \sigma = \rho_1 \circ \rho_2 \circ ... \circ \rho_s$$

Então os inteiros $r$ e $s$ têm a mesma paridade.

*Demonstração:* Devido ao corolário 1, $\text{sgn}\ \sigma = (-1)^r = (-1)^s$. Se $r$ for par, então $(-1)^r = 1$; daí $(-1)^s = 1$ e, portanto, $s$ também é par. O raciocínio é análogo no caso em que $r$ é ímpar. #

**Definição 16:** Uma permutação $\sigma \in S_n$ é chamada *par* ou *ímpar* conforme possa ser expressa como um produto de um número par ou ímpar de transposições. Em outras palavras, conforme sua assinatura seja $+1$ ou $-1$. O conjunto das permutações pares de $S_n$ será indicado por $A_n$. $A_n \neq \varnothing$ pois $\varepsilon = (12)(21)$ é par.

**Proposição 32:** Para todo $n > 1$, o conjunto $A_n$ é um subgrupo, de ordem $n!/2$ e índice 2, de $S_n$.

O subgrupo $A_n$ será chamado *grupo alternado* de grau $n$.

*Demonstração:* Sejam $\sigma, \varphi \in A_n$. Então $\text{sgn}\ (\sigma) = 1$ e $\text{sgn}\ \varphi = 1$. Como, porém, $\text{sgn}\ (\sigma \circ \varphi^{-1}) = (\text{sgn}\ \sigma)(\text{sgn}\ \varphi)^{-1} = 1 \cdot 1^{-1} = 1$, então $\sigma \circ \varphi^{-1} \in A_n$. Fica provado, pois, que $A_n$ é um subgrupo de $S_n$.

Sejam $r$ as permutações pares e $s$ as permutações ímpares de $S_n$, que denotaremos respectivamente por $\sigma_1, \sigma_2, ..., \sigma_r$ e $\varphi_1, \varphi_2, ..., \varphi_s$. Multiplicando as permutações pares por uma transposição $\tau$, obtemos as permutações:

$$\tau \circ \sigma_1, \tau \circ \sigma_2, ..., \tau \circ \sigma_r$$

Como todo elemento de um grupo é regular, o número desses produtos também é $r$. Mas, como o produto de uma permutação ímpar (a transposição $\tau$) por uma par, todos esses produtos são ímpares. Logo, $r \leqslant s$.

Analogamente, se multiplicarmos as permutações ímpares por $\tau$, obteremos as $s$ permutações pares:

$$\tau \circ \varphi_1, \tau \circ \varphi_2, ..., \tau \circ \varphi_s$$

Portanto, $s \leqslant r$. De onde, $r = s$, e como $r + s = n!$, então $o(A_n) = \dfrac{n!}{2}$ e, por conseguinte, $(S_n : A_n) = 2$. #

**Corolário:** $A_n$ é um subgrupo normal de $S_n$. (Ver exemplo 41.)

*Exemplo 51:* Achar todas as permutações pares de $S_3$. Lembremos que $S_3 = \left\{ f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$
$\left. g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$.

Então, $f_0$ é par, $f_1 = (1\ \ 2\ \ 3) = (1\ \ 3) \circ (1\ \ 2)$ é par, $f_2 = (1\ \ 3\ \ 2) = (1\ \ 2) \circ (1\ \ 3)$ é par, $g_1 = (2\ \ 3)$ é ímpar, $g_2 = (1\ \ 3)$ é ímpar e $g_3 = (1\ \ 2)$ é ímpar. Logo, o grupo alternado neste caso é:

$$A_3 = \{f_0, f_1, f_2\}$$

*Exemplo 52.* Construir a tábua do grupo $S_n/A_n$

Como vimos, $o(A_n) = (S_n : A_n) = 2$ e, então, $S_n/A_n = \{A_n, \varphi A_n\}$, em que $\varphi$ é uma permutação ímpar qualquer. Uma maneira de construir a tábua pedida é lembrar que todos os grupos de ordem 2 são isomorfos. Então.

| $\cdot$ | $A_n$ | $\varphi A_n$ |
|---|---|---|
| $A_n$ | $A_n$ | $\varphi A_n$ |
| $\varphi A_n$ | $\varphi A_n$ | $A_n$ |

## Exercícios

**135.** Dê um exemplo de duas permutações do grupo $S_3$ que não comutam.

**136.** Expresse cada uma das seguintes permutações de $S_8$ como produto de ciclos disjuntos e, depois, como produto de transposições:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$

**137.** Qual é a inversa da permutação $\sigma = (1\ \ 2)\ (3\ \ 5)\ (7\ \ 8\ \ 9)$ no grupo $S_{10}$?

**138.** Determine as assinaturas das seguintes permutações:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$

d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

**139.** Responda às seguintes perguntas referentes ao grupo $S_8$:

a) Qual a ordem do ciclo $(1\ \ 4\ \ 5\ \ 7)$?

b) Qual a ordem de $(4\ \ 5)\ (2\ \ 3\ \ 7)$?

**140.** Decomponha cada uma das seguintes permutações num produto de ciclos disjuntos dois a dois e determine suas ordens e assinaturas.

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 8 & 6 & 3 & 4 & 9 & 1 & 2 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

**141.** Encontre a ordem de cada um dos elementos de $S_4$:

a) $(1 \quad 2 \quad 3)$

b) $(1 \quad 4 \quad 3 \quad 2)$

c) $(1 \quad 2)(3 \quad 4)$

**142.** Determine todas as permutações de $S_{10}$ que são permutáveis com $(1 \quad 2 \quad 3 \quad 4 \quad 5)(6 \quad 7 \quad 8 \quad 9 \quad 10)$.

**143.** Construa uma tábua do grupo alternado $A_4$.

**144.** Se $\sigma \in S_n$ é um ciclo de comprimento $r$, mostre que $o(\sigma) = r$.

**145.** Sejam $\sigma, \varphi \in S_n$ ciclos disjuntos. Mostre que $o(\sigma \circ \varphi) = \text{mmc}\,(o(\sigma), o(\varphi))$.

**Resolução**

Sejam $r$, $s$ e $t$, respectivamente, as ordens de $\sigma$, $\varphi$ e $\sigma \circ \varphi$ e $m = \text{mmc}\,(r, s)$. Lembremos as propriedades que caracterizam $m$: (i) $m \geqslant 0$; (ii) $r \mid m$ e $s \mid m$; (iii) se $m'$ é um inteiro tal que $r \mid m'$ e $s \mid m'$, então $m \mid m'$.

Como $m$ é múltiplo de $r$ e $s$ e $\sigma$ e $\varphi$ comutam entre si, então $(\sigma \circ \varphi)^m = \sigma^m \circ \varphi^m = \varepsilon \circ \varepsilon = \varepsilon$ e, então, devido à proposição 17, $t \mid m$.

Por outro lado, $(\sigma \circ \varphi)^t = \sigma^t \circ \varphi^t = \varepsilon$, pois a ordem de $\sigma \circ \varphi$ é $t$. Agora, se $a$ é um elemento do suporte de $\sigma$, então $\varphi(a) = a$ e, portanto, $\varphi^t(a) = a$. Então $\sigma^t(a) = (\sigma^t \circ \varphi^t)(a) = \varepsilon(a) = a$ e daí segue, devido à proposição citada, que $r \mid t$. Analogamente se demonstra que $s \mid t$. Portanto, $m \mid t$. Como já provamos que $t \mid m$, então $m = t$. ■

**146.** Mostre que o número de permutações ímpares de $\{1, ..., n\}$, para $n \geqslant 2$, é igual ao número de permutações pares.

**147.** Mostre que a assinatura do $r$-ciclo $(a_1 \; a_2 \; ... \; a_r)$ é $(-1)^{r+1}$.
*Sugestão:* Use o método da indução finita.

**148.** Seja $\sigma$ um ciclo de comprimento $r$ Se $r$ é ímpar, mostre que $\sigma^2$ também é um ciclo.

**149.** Justifique as seguintes identidades:

a) $(1\ \ 2\ \ \dots\ \ k) = (1\ \ 2\ \ \dots\ \ j) \circ (j\ \ j+1\ \ \dots\ \ k)\quad (1 < j < k)$

b) $(1\ \ 2\ \ \dots\ \ k) = (1\ \ k)\ \ (1\ \ 2\ \ \dots\ \ k-1)\quad (k > 1)$

c) $(1\ \ 2\ \ \dots\ \ k) \circ (k-1\ \dots\ 2\ \ 1) = (1\ \ k)$

**150.** Prove que $(a_1\ \ a_2\ \ \dots\ \ a_k)^{-1} = (a_k\ \ a_{k-1}\ \ \dots\ \ a_2\ \ a_1)$.

**151.** Sejam $\sigma, \varphi \in S_n$ ciclos disjuntos tais que $\sigma \circ \varphi = \varepsilon$. Prove que $\sigma = \varphi = \varepsilon$.

**Resolução**

Seja $\varphi = (a_1\ \ a_2\ \ \dots\ \ a_r)$. Portanto, $\varphi(a_1) = a_2$. Mas, sendo disjuntos os ciclos dados, $a_2$ não pertence ao suporte de $\sigma$ e, portanto, $\sigma(a_2) = a_2$. Como, porém, $\sigma \circ \varphi = \varepsilon$, então $(\sigma \circ \varphi)(a_1) = a_1$. Mas $(\sigma \circ \varphi)(a_1) = (\sigma)(\varphi(a_1)) = \sigma(a_2) = a_2$. Logo, $a_2 = a_1$. Esse raciocínio, estendido a todos os elementos do suporte de $\varphi$, levará à conclusão de que $a_1 = a_2 = \dots = a_r$ e, portanto, de que $\varphi$ é a permutação idêntica. Como, por hipótese, $\sigma \circ \varphi = \varepsilon$ e $\varphi = \varepsilon$, pelo que acabamos de provar, então $\sigma = \varepsilon$. ■

**152.** Sejam $\sigma, \varphi \in S_n$. Prove que $\text{sgn}\ \sigma = \text{sgn}\ (\varphi \circ \sigma \circ \varphi^{-1})$.

**153.** Mostre que em $S_n$, se $\sigma$ comuta com a permutação circular $\tau = (1\ \ \ 2\ \ \dots\ \ n)$, então $\sigma = \tau^i$ com $i \in \mathbb{Z}^*$.

CAPÍTULO V

# ANÉIS E CORPOS

## V-1 ANÉIS

### 1. NOTA HISTÓRICA

Um aspecto que chama a atenção na história da álgebra é seu desenvolvimento tardio no que se refere à organização lógica e axiomatização. Considerando-se que a geometria já recebera uma axiomatização nos *Elementos* de Euclides (c. 300 a.C.), o fato de datar do século XIX a primeira tentativa feita nesse sentido para a álgebra põe em relevo dificuldades teóricas de grande porte. Além do mais, a obra em que aparece a primeira tentativa de axiomatização da álgebra, do inglês Benjamin Peacock (1791-1858), publicada em 1830, em pouco tempo foi totalmente superada.

Pouco depois disso, o irlandês William R. Hamilton (1805-1865) engajou-se na tarefa de criar um sistema numérico que desempenhasse no espaço tridimensional o mesmo papel, algebricamente falando, que o sistema dos números complexos desempenha no espaço bidimensional (o plano). Inicialmente o matemático imaginou que esses novos números seriam do tipo $a + bi + cj$ (com $i^2 = j^2 = -1$). Mas em 1843, depois de mais de dez anos de pesquisas, descobriu que eles tinham de ser do tipo $a + bi + cj + dk$ (com $i^2 = j^2 = k^2 = -1$) e que teria de abrir mão da comutatividade da multiplicação. A criação desses novos números, os *quaternions*,

mostrou que as leis clássicas da álgebra (como a comutatividade) podem não ser aplicáveis em certos casos. O trabalho de Hamilton e outros matemáticos colaborou, já no século XIX, para a criação de inúmeras "estruturas algébricas" novas, entre as quais as de "corpo" e de "anel".

Na verdade, o embrião da idéia de corpo já aparecera nos anos 1820, nos trabalhos sobre equações algébricas do norueguês N. H. Abel (1802-1829). Abel entendia por corpo uma coleção de números fechada para a adição, subtração, multiplicação e divisão (salvo no caso de divisor igual a zero). Mas a idéia de corpo só se tornaria explícita quando o alemão R. Dedekind (1831-1916) introduziu os *corpos de números de grau finito* como base para o estudo dos *números algébricos*.

Um número complexo se diz *algébrico* se é raiz de um polinômio com coeficientes racionais. Por exemplo, $\sqrt{2}/2$ é algébrico, pois é raiz de $p(x) = 2x^2 - 1$. Um número complexo que não é algébrico diz-se *transcendente*. Os exemplos mais notáveis de números transcendentes são $\pi$ e $e$. Demonstra-se que, se $\alpha$ e $\beta$ são algébricos, também o são $a \pm \beta$, $a\beta$ e $a/\beta$ (se $\beta \neq 0$) e, portanto, o sistema dos números algébricos é um corpo, segundo a idéia de Abel. Porém, o primeiro matemático a dar uma definição abstrata de corpo foi H. Weber (1842-1913), num artigo de 1893.

Essas pesquisas levaram naturalmente à idéia de *inteiro algébrico*. Um numero complexo se diz *inteiro algébrico* se é raiz de um polinômio cujo coeficiente do termo de maior grau é 1 e os demais são números inteiros. Por exemplo, o número $i$ e um inteiro algébrico, pois é raiz de $p(x) = x^2 + 1$. Demonstra-se que, se $\alpha$ e $\beta$ são inteiros algébricos, então $\alpha + \beta$ e $\alpha\beta$ também o são. Mas $\alpha/\beta$ não é necessariamente inteiro algébrico, mesmo quando $\beta \neq 0$. Nessas propriedades, compartilhadas pelo sistema dos numeros inteiros, inspira se a definição de anel. Mas a primeira definição abstrata de anel (ver **2.1**) só seria dada em 1914 pelo alemão A. Fraenkel (1891-1965), embora o nome *anel* já tivesse sido introduzido por D. Hilbert (1852-1943) perto do final do século XIX.

## 2. ANÉIS E SUBANÉIS

### 2.1 Conceito de anel

**Definição 1:** Um sistema matemático constituído de um conjunto não vazio $A$ e um par de operações sobre $A$, respectivamente uma adição $(x, y) \mapsto x + y$ e uma multiplicação $(x, y) \mapsto xy$ (ou $x \cdot y$), é chamado *anel* se:

(i) $(A, +)$ é um grupo abeliano, ou seja:

(a) se $a, b, c \in A$, então $a + (b + c) = (a + b) + c$ (associatividade);

(b) se $a, b \in A$, então $a + b = b + a$ (comutatividade);

(c) existe um elemento $0_A \in A$ tal que, qualquer que seja $a \in A$, $a + 0_A = a$ (existência de elemento neutro);

(d) qualquer que seja $a \in A$, existe um elemento em $A$, indicado genericamente por $-a$, tal que $a + (-a) = 0_A$ (existência de opostos).

(ii) A multiplicação goza da propriedade associativa, isto é:

se $a, b, c \in A$, então $a(bc) = (ab)c$.

(iii) A multiplicação é distributiva em relação à adição, vale dizer:

se $a, b, c \in A$, então $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$.

Por uma questão de simplicidade de linguagem, poderemos identificar a adição do anel com o símbolo $+$ e a multiplicação com um ponto. E, quando não houver possibilidade de confusão, até esses símbolos poderão ser omitidos. Por exemplo, será comum usarmos expressões como "Seja $(A, +, \cdot)$ um anel" ou mesmo "Seja $A$ um anel" ou "Consideremos um anel $A$". Naturalmente as duas últimas alternativas pressupõem que não haja confusão possível quanto às operações subentendidas. Outra maneira simplificada de nos referirmos a um anel $A$ será dizendo que "$A$ tem uma estrutura de anel", o que naturalmente também pressupõe as operações já subentendidas.

## 2.2 Propriedades imediatas de um anel

Seja $(A, +, \cdot)$ um anel.

(a) As propriedades aqui reunidas são conseqüências do fato de que a adição é uma operação sobre $A$ e de que $(A, +)$ é um grupo aditivo abeliano:

- O elemento neutro $0_A$ é único. Esse elemento é chamado *zero* do anel e, quando não houver possibilidade de confusão, poderá ser indicado apenas pelo símbolo 0.
- O oposto $-a$ de um elemento $A$ do anel é único.
- Se $a_1, a_2, ..., a_n \in A$, então $-(a_1 + a_2 + ... + a_n) = (-a_1) + (-a_2) + ... + (-a_n)$. (Observar que a comutatividade da adição foi usada.)
- Se $a \in A$, então $-(-a) = a$.
- Se $a + x = a + y$, então $x = y$. Ou seja, todo elemento de $A$ é regular para a adição. Ou, dito em outros termos, vale a *lei do cancelamento da adição*.
- A equação $a + x = b$ tem uma e uma só solução: o elemento $b + (-a)$.

(b) Se $a \in A$, então $a \cdot 0 = 0 \cdot a = 0$.

*Justificação:*

$$0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

(cancelando $a \cdot 0$)

$$0 = a \cdot 0$$

Analogamente se demonstra que $0 \cdot a = 0$. #

(c) Se $a, b \in A$, então $a(\ \ b) \quad (\ \ a)b \qquad (ab)$.

*Justificação:*

$$\underline{ab + [-(ab)]} = 0 = a \cdot 0 \quad a[b + (\ \ b)] = \underline{ab + a(\ \ b)}$$

(cancelando $ab$)

$$\downarrow$$

$$-(ab) = a(-b)$$

Analogamente se demonstra que $\quad (ab) = (\ \ a)b$. #

(d) Se $a, b \in A$, então $(-a)(-b) = ab$.

*Justificação:* Devido à propriedade anterior, $(-a)(-b) = -[a(-b)]$. Pelo mesmo motivo, $a(-b) = -(ab)$. Portanto:

$$(-a)(-b) = -[-(ab)] = ab \ \#$$

**Definição 2** (diferenças em um anel): Sejam $a, b \in A$. Chama-se *diferença* entre $a$ e $b$ e indica-se por $a - b$ o elemento $a + (-b) \in A$. Portanto, $a - b = a + (-b)$.

(e) Se $a, b \in A$, então $a(b - c) = ab - ac$ e $(a - b)c = ac - bc$.

*Justificação:* $a(b - c) = a[b + (-c)] = ab + a(-c)$. Como, porém, $a(-c) = -ac$, então:

$$a(b - c) = ab + (-ac) = ab - ac$$

Deixamos como exercício a demonstração de que $(a - b)c = ac - bc$. #

## 2.3 Alguns anéis importantes

(i) *Anéis numéricos*

São os mais importantes. As operações são as usuais, cujas propriedades, como é bem conhecido, cumprem os axiomas da definição:

- *anel dos números inteiros*: $(\mathbb{Z}, +, .)$;
- *anel dos números racionais*: $(\mathbb{Q}, +, .)$;
- *anel dos números reais*: $(\mathbb{R}, +, .)$;
- *anel dos números complexos*: $(\mathbb{C}, +, .)$.

(ii) *Anel das classes de resto módulo* m

Para todo inteiro $m > 1$, é o conjunto $\mathbb{Z}_m \quad \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m \quad 1}\}$ em relação às operaçoes assim definidas:

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{e} \quad \bar{a} \cdot \bar{b} = \overline{ab}$$

As propriedades dessas operações, estudadas no capítulo III, garantem que real mente se trata de anéis. Apenas lembramos que o zero desse anel é a classe $\bar{0}$ e que o oposto de um elemento $\bar{a} \in \mathbb{Z}_m$ é a classe $m \qquad a$.

Para simplificar, poderemos trabalhar eventualmente com um conjunto $\mathbb{Z}_m$ sem

usar os traços sobre seus elementos. Ou seja, poderemos escrever simplesmente:

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$$

Mas, quando isso acontecer, deve-se lembrar que:

$a + b$ = resto da divisão de $a + b$ por $m$

e

$ab$ = resto da divisão de $ab$ por $m$

Por exemplo, no anel $\mathbb{Z}_{12}$:

$$9 + 11 = 8 \quad \text{e} \quad 9 \cdot 11 = 3$$

(iii) *Anéis de matrizes*

Entre os exemplos de grupos aditivos dados no capítulo precedente, figuravam os das matrizes $m \times n$ sobre $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, todos comutativos. E, entre os grupos multiplicativos, os grupos lineares de grau $n$, cujos elementos são as matrizes quadradas racionais, reais ou complexas inversíveis (determinante não nulo), nenhum deles comutativo, salvo no caso em que $n = 1$.

Como se trata agora de introduzir os anéis de matrizes, a partir desses grupos, e, portanto, as duas operações devem ser consideradas simultaneamente, então só interessam as matrizes quadradas. Lembrando as propriedades da adição e da multiplicação de matrizes quadradas e que da definição de anel não faz parte o axioma da existência de inversos, podemos concluir que, para qualquer inteiro $n > 0$, são anéis:

$$(M_n(\mathbb{Z}), +, \cdot), (M_n(\mathbb{Q}), +, \cdot), (M_n(\mathbb{R}), +, \cdot), (M_n(\mathbb{C}), +, \cdot)$$

respectivamente *anel das matrizes inteiras, racionais, reais* e *complexas*, de ordem $n$.

Pode-se ir mais longe, porém. Se $A$ é um anel, não importa qual a natureza de seus elementos, então pode-se construir o conjunto $(M_n(A), +, \cdot)$ das matrizes $n \times n$ sobre $A$, para todo $n \geqslant 1$, de maneira análoga ao que é feito nos casos numéricos. E estender para essas matrizes a adição e a multiplicação do anel. No caso de $(M_2(\mathbb{Z}_3), +, \cdot)$, por exemplo, se

$$B = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{2} & \bar{1} \end{pmatrix} \quad \text{e} \quad C = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{2} & \bar{1} \end{pmatrix}$$

então:

$$B + C = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{2} \end{pmatrix} \quad \text{e} \quad BC = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$$

Não é difícil provar que, nessas condições, $(M_n(A), +, \cdot)$ também é um anel: o *anel das matrizes sobre A de ordem* n.

(iv) *Anéis de funções*

Seja $A = \mathbb{Z}^{\mathbb{Z}} = \{f \mid f\colon \mathbb{Z} \to \mathbb{Z}\}$. Se $f, g \in A$, define-se a *soma* $f + g$ e o *produto* de $fg$ dessas funções da seguinte maneira:

$f + g\colon \mathbb{Z} \to \mathbb{Z}$ e $(f + g)(x) = f(x) + g(x)$, para todo $x \in \mathbb{Z}$;

$fg\colon \mathbb{Z} \to \mathbb{Z}$ e $(fg)(x) = f(x)g(x)$, para todo $x \in \mathbb{Z}$.

Isso posto, pode se mostrar que o terno constituído pelo conjunto $A$ e as operações $(f, g) \in A \times A \mapsto f + g \in A$ (*adição*) e $(f, g) \in A \times A \mapsto fg \in A$ (*multiplicação*) é um anel, o *anel das funções de $\mathbb{Z}$ em $\mathbb{Z}$*. Por brevidade, e até porque a dificuldade envolvida é pequena, nos deteremos na justificação de apenas dois dos axiomas da definição de anel.

• O zero do anel, como seria de esperar, é a função $0_A: \mathbb{Z} \to \mathbb{Z}$ definida por $0_A(x) = 0$ (número zero). De fato, $(f + 0_A)(x) = f(x) + 0_A(x) = f(x) + 0 = f(x)$, qualquer que seja $x \in \mathbb{Z}$. Portanto, se $f \in A$, então $f + 0_A = f$.

• Provemos a propriedade distributiva da multiplicação em relação à adição. Se $f, g, h \in A$, então, qualquer que seja $x \in \mathbb{Z}$:

$$[f(g + h)](x) = f(x)[(g + h)(x)] = f(x)[g(x) + h(x)] =$$
$$= f(x)g(x) + f(x)h(x) = (fg)(x) + (fh)(x) = (fg + fh)(x)$$

Portanto, $f(g + h) = fg + fh$. Analogamente se demonstra que $(f + g)h = fh + gh$. (Isso, aliás, seria desnecessário, observando-se que a multiplicação é comutativa.)

Da mesma forma introduzem-se os anéis $\mathbb{Q}^{\mathbb{Q}}$, $\mathbb{R}^{\mathbb{R}}$ e $\mathbb{C}^{\mathbb{C}}$. De modo geral, se $A$ é um anel e $X$ é um conjunto não vazio, então pode-se transformar $A^X$ em anel, definindo-se adição e multiplicação de funções de $X$ em $A$ de maneira análoga ao que foi feito em $\mathbb{Z}^{\mathbb{Z}}$.

Por exemplo, se $X = \{a, b\}$ e $A = \mathbb{Z}_2 = \{0, 1\}$, então o anel $A$ das aplicações de $X$ em $\mathbb{Z}_2$ é constituído de 4 elementos, as funções $f, g, h, u$, definidas respectivamente pelas seguintes relações:

$f(a) = 0$ e $f(b) = 0$, $g(a) = 1$ e $g(b) = 1$, $h(a) = 0$ e $h(b) = 1$; $u(a) = 1$ e $u(b) = 0$

A título de ilustração, ressaltemos o seguinte:

• o zero desse anel é a aplicação $f$;

• $-g = g$, pois $(g + g)(x) = g(x) + g(x) = 1 + 1 = 0$ e, portanto, $g + g = f$ (zero do anel);

• $-h = h$ (raciocínio análogo);

• $-u = u$ (raciocínio análogo).

(v) *Produtos diretos*

Sejam $A$ e $B$ anéis e consideremos o produto cartesiano $A \times B$. Há uma maneira, por assim dizer, natural de transformar esse produto em um anel, que é definindo-se a adição e a multiplicação componente a componente. Ou seja:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

e

$$(a_1, b_1) + (a_2, b_2) = (a_1a_2, b_1b_2)$$

A verificação de que efetivamente $(A \times B, +, \cdot)$ é um anel é rotineira. Por exemplo, o zero do anel $A \times B$ é o par $(0_A, 0_B)$, em que $0_A$ é o zero de $A$ e $0_B$ é o zero de $B$,

pois $(a, b) + (0_A, 0_B) = (a + 0_A, b + 0_B) = (a, b)$. Segue, como exemplo, a demonstração da associatividade da multiplicação:

$$[(a_1, b_1)(a_2, b_2)](a_3, b_3) = (a_1a_2, b_1b_2)(a_3, b_3) = ((a_1a_2)a_3, (b_1b_2, b_3) \overset{*}{=}$$
$$\overset{*}{=} (a_1(a_2a_3), b_1(b_2b_3)) = (a_1, b_1)(a_2a_3, b_2b_3) = (a_1, b_1)[(a_2, b_2)(a_3, b_3)]$$

Notar que na passagem * usou-se a associatividade em $A$ e $B$, nas demais, a definição de produto.

## 2.4 Anéis finitos

Um anel $(A, +, \cdot)$ em que o conjunto $A$ é finito chama-se *anel finito*. Os anéis $\mathbb{Z}_m$ $(m > 1)$ são exemplos importantes de anéis finitos. Também são finitos os anéis $A^M$, sempre que $A$ é um anel finito e $M$ um conjunto finito. Neste caso, se $a$ indica o número de elementos de $A$ e $m$ o número de elementos de $M$, então $A^M$ tem $a^m$ elementos.

Se $A$ é um anel finito, as tábuas da adição e da multiplicação podem ser instrumentos úteis para visualizar algumas de suas características. Como exemplo, vamos construir as tábuas do anel $\mathbb{Z}_4 = \{0, 1, 2, 3\}$:

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| · | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

A tábua da multiplicação revela que esse anel não segue totalmente as leis clássicas da álgebra. Notemos, por exemplo, o seguinte:

$2 \cdot 2 = 0$ (zero do anel) sem que os fatores sejam iguais a 0;

$2 \cdot 1 = 2 \cdot 3$ e não é possível cancelar o 2, mesmo se tratando de um elemento diferente do zero do anel.

## 2.5 Subanéis

**Definição 3:** Sejam $(A, +, \cdot)$ um anel e $L$ um subconjunto não vazio de $A$. Diz-se que $L$ é um subanel de $A$ se:

(i) $L$ é fechado para as operações que dotam o conjunto $A$ da estrutura de anel;

(ii) $(L, +, \cdot)$ também é um anel. (Naturalmente a adição e a multiplicação consideradas sao as mesmas de $A$, porém restritas aos elementos de $L$.)

*Exemplo 1.* Considerando-se as operações usuais sobre os conjuntos numéricos: $\mathbb{Z}$ é subanel de $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{Q}$ é subanel de $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{R}$ é subanel de $\mathbb{C}$

*Exemplo 2:* $M_n(\mathbb{Z})$ é subanel de $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$; $M_n(\mathbb{Q})$ é subanel de $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$, $M_n(\mathbb{R})$ é subanel de $M_n(\mathbb{C})$.

**Proposição 1:** Sejam $A$ um anel e $L$ um subconjunto não vazio de $A$. Então $L$ é um subanel de $A$ se, e somente, se $a - b$, $ab \in L$, sempre que $a, b \in L$.

*Demonstração:*

($\rightarrow$) Seja $L$ um subanel de $A$. Da definição decorre que $L$ é um subgrupo do grupo abeliano $A$. Portanto, $a - b \in L$ sempre que $a, b \in L$. Completando, a própria definição impõe que $ab \in L$ sempre que $a, b \in L$.

($\leftarrow$) Por hipótese, se $a, b \in L$, então $a - b \in L$. Isso prova que $L$ é um subgrupo do grupo aditivo $A$ (proposição 1, capítulo IV). Por outro lado, considerando-se que, por hipótese, $L$ é fechado para a multiplicação:

— se $a, b, c \in L$, então $a, b, c \in A$ e, portanto, $a(bc) = (ab)c$, o que demonstra a associatividade da multiplicação em $L$;

— se $a, b, c \in L$, então $a, b, c \in A$ e, portanto, $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$, o que demonstra que, em $L$, a multiplicação é distributiva em relação à adição. #

Lembremos o seguinte: (i) se $A$ é um anel, então $A$ é um grupo aditivo; (ii) um subconjunto não vazio de um grupo aditivo é um subgrupo desse grupo se, e somente se, é fechado para a subtração. Então a proposição anterior pode ser formulada nos seguintes termos:

"Sejam $A$ um anel e $L$ um subconjunto não vazio de $A$. Então $L$ é um subanel de $A$ se, e somente se, $L$ é um subrupo do grupo aditivo $(A, +)$ e $ab \in L$, quaisquer que sejam os elementos $a, b \in L$."

*Exemplo 3:* $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. $L$ é um subanel de $\mathbb{R}$, pois, se $a + b\sqrt{2}$, $c + d\sqrt{2} \in L$, então:

$$\left(a + b\sqrt{2}\right) - \left(c + d\sqrt{2}\right) = (a - c) + (c - d)\sqrt{2} \in L$$
$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2} \in L$$

Esse subanel de $\mathbb{R}$ costuma ser denotado por $\mathbb{Z}\left[\sqrt{2}\right]$.

*Exemplo 4:* Consideremos o anel $A = \mathbb{R}^{\mathbb{R}}$ das funções reais de uma variável real. Seja $L = \{f \in A \mid f(1) = 0\}$. $L$ é um subanel de $A$, porque não é um conjunto vazio (a função $h: \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x - 1$, por exemplo, pertence a $L$) e, se $f, g \in L$, então:

$$(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$$

e

$$(fg)(1) = f(1)g(1) = 0 \cdot 0 = 0$$

o que significa que $f - g, fg \in L$.

*Exemplo 5:* Seja $L$ um subconjunto não vazio de $\mathbb{Z}$. Então $L$ é subanel de $\mathbb{Z}$ (operações usuais) se, e somente se, $L$ é um subgrupo do grupo aditivo $\mathbb{Z}$.

A própria definição de subanel garante, como já ressaltamos na demonstração da proposição 1, que, se $L$ é um subanel de $\mathbb{Z}$, então $L$ é um subgrupo de $\mathbb{Z}$.

Reciprocamente, seja $L$ um subgrupo do grupo aditivo $\mathbb{Z}$. Mas, como já vimos, $L$ é cíclico, pelo fato de $\mathbb{Z}$ ser um grupo aditivo cíclico. Então $L = [a] = \{0, \pm a, \pm 2a, ...\}$, para algum $a \in L$. Isso posto, se $x, y \in L$, então $x = sa$ e $y = ta$, para convenientes inteiros $s$ e $t$ e, portanto, $x - y = (s - t)a \in L$ e $xy = (sta)a \in L$. A proposição 1 nos garante, então, que $L$ é subanel de $\mathbb{Z}$.

Esse resultado, visto por outro ângulo, diz o seguinte: $L$ é subanel de $\mathbb{Z}$ se, e somente se, existe $n \in L$ tal que $L = \{0, \pm n, \pm 2n, ...\}$. Na teoria dos anéis, o conjunto dos múltiplos inteiros de um elemento $n \in \mathbb{Z}$ às vezes é indicado por $n\mathbb{Z}$.

## 3. TIPOS DE ANÉIS

A definição de anel é bastante aberta no que se refere à multiplicação. Por exemplo, há anéis que possuem elemento neutro para a multiplicação e outros que não. O anel $\mathbb{Z}$, por exemplo, possui elemento neutro para a multiplicação: o número 1. Já o anel $2\mathbb{Z} = \{0, \pm 2, \pm 4, ...\}$ (que é um subanel de $\mathbb{Z}$), não.

Da mesma forma, há anéis cuja multiplicação é comutativa e outros em que isso não acontece. Por exemplo, a multiplicação do anel dos inteiros goza da propriedade comutativa. Mas, no anel $M_n(\mathbb{R})$, por exemplo, isso não acontece, salvo quando $n = 1$. E há outros aspectos em relação aos quais os anéis podem ser subdivididos. Um dos objetivos em vista agora é explorar toda essa abertura propiciada pelos axiomas referentes à multiplicação.

### 3.1 Anéis comutativos

**Definição 4:** Seja $A$ um anel. Se a multiplicação de $A$ goza da propriedade comutativa, isto é, se

$$ab = ba$$

para quaisquer $a, b \in A$, então se diz que $A$ é um *anel comutativo*.

*Exemplo 6:* Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ cuja multiplicação é sabidamente comutativa.

*Exemplo 7:* Os anéis $\mathbb{Z}_m$ das classes de resto, módulo $m$. De fato, se $a, b \in \mathbb{Z}_m$, então $ab = ba$ (multiplicação módulo $m$), pois o resto da divisão de $ab$ por $m$ é igual ao resto da divisão de $ba$ por $m$.

*Exemplo 8:* Os anéis de funções $A^X$, sempre que $A$ é um anel comutativo. Realmente, se $f, g \in A^X$ e se $x$ é um elemento genérico de $X$, então.

$$(fg)(x) \overset{*}{=} f(x)g(x) \overset{**}{=} g(x)f(x) \overset{*}{=} (gf)(x)$$

Portanto, $fg = gf$.

Notar que nas passagens assinaladas com * usamos a definição de produto de funções e na passagem assinalada com ** a comutatividade da multiplicação em $A$. #

*Contra-exemplo 1:* Não são comutativos os anéis $M_n(A)$, em que $A$ indica $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, se $n > 1$. De fato, como já vimos (exemplo ix, **2.4**, capítulo IV), se $n > 1$ e

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

então $AB \neq BA$.

## 3.2 Anéis com unidade

**Definição 5:** Seja $A$ um anel. Se $A$ conta com elemento neutro para a multiplicação, isto é, se existe um elemento $1_A \in A$, $1_A \neq 0_A$, tal que

$$a \cdot 1_A = 1_A \cdot a = a$$

qualquer que seja $a \in A$, então se diz que $1_A$ é a *unidade* de $A$ e que $A$ é um *anel com unidade*. Quando não houver possibilidade de confusão, poderemos indicar a unidade simplesmente pelo símbolo 1.

*Exemplo 9:* Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ cuja unidade é o número 1.

*Exemplo 10:* Os anéis $\mathbb{Z}_m$ das classes de resto módulo $m$. A unidade é a classe $\overline{1}$, pois $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$ e $\mathbb{Z}_m$ é comutativo.

*Exemplo 11:* Os anéis $M_n(A)$, em que $A$ é um dos anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. A unidade é a matriz

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

*Exemplo 12:* Se $A$ é um anel com unidade, então a aplicação constante $u: X \to A$, $u(x) = 1_A$, é a unidade do anel $A^X$. De fato, para qualquer $f \in A^X$ e qualquer $x \in X$: $(f \cdot u)(x) = f(x)u(x) = f(x) \cdot 1_A = f(x)$. Portanto, $f \cdot u = f$. Analogamente se demonstra que $u \cdot f = f$. Isso mostra que, se $A$ é um anel com unidade, o mesmo ocorre com $A^X$.

*Contra-exemplo 2:* Os anéis $n\mathbb{Z}$ não possuem unidade quando $n \neq \pm 1$. Consideremos, por exemplo, o caso em que $n = 2$, ou seja, consideremos o anel $2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$. A unidade, se existisse, seria um número par $2x_0$ tal que $a \cdot (2x_0) = a$ para todo $a \in 2\mathbb{Z}$. Mas isso implica $2x_0 = 1$, igualdade impossível em $2\mathbb{Z}$.

**Definição 6** (potências num anel): Seja $A$ um anel com unidade. Se $a \in A$ e $n$ é um número natural, define-se $a^n$ (potência $n$-ésima de $A$) por recorrência da seguinte maneira:

$$a^0 = 1_A \quad \text{e} \quad a^{n+1} = a^n a \text{ (sempre que } n \geq 0)$$

**Proposição 2:** Seja $A$ um anel com unidade. Se $a \in A$ e $m$, $n$ são números naturais, então: (i) $a^m a^n = a^{m+n}$; (ii) $(a^m)^n = a^{mn}$.

*Demonstração:*

(i) (Por indução sobre $n$)

Se $n = 0$, então $a^m a^0 = a^m \cdot 1_A = a^m = a^{m+0}$. Portanto, a propriedade vale para $n = 0$.

Seja $r \geq 0$ um número natural e suponhamos $a^m a^r = a^{m+r}$.

Então: $a^m a^{r+1} \overset{*}{=} a^m(a^r a) \overset{**}{=} (a^m a^r)a \overset{***}{=} (a^{m+r})a \overset{*}{=} a^{(m+r)+1}$.

Portanto, se a propriedade vale para $r \geq 0$, vale também para $r + 1$. De onde, pelo primeiro princípio de indução, vale para todo $n \geq 0$.

Observar que nas passagens assinaladas com * usamos a definição; na passagem assinalada com **, a associatividade da multiplicação; e na passagem assinalada com ***, a hipótese de indução.

(ii) (Por indução sobre $n$)

Se $n = 0$, então $(a^m)^0 = 1_A = a^0 = a^{m \cdot 0}$. Portanto, a propriedade vale para $n = 0$.

Seja $r \geq 0$ um número natural e suponhamos $(a^m)^r = a^{mr}$.

Então, $(a^m)^{r+1} \overset{*}{=} (a^m)^r a^m \overset{**}{=} a^{mr} a^m \overset{***}{=} a^{mr+m} = a^{m(r+1)}$.

Portanto, se a propriedade vale para $r \geq 0$, vale também para $r + 1$. De onde, pelo primeiro princípio de indução, vale para todo $n \geq 0$.

Observar que na passagem * usamos a definição; na ** a hipótese de indução, e na *** a propriedade anterior. #

Seja $A$ um anel com unidade e $L$ um subanel de $A$. As seguintes possibilidades podem ocorrer:

- $L$ possui unidade e essa unidade é a mesma de $A$. É o que ocorre, por exemplo, com o anel $\mathbb{Z}$ dos inteiros como subanel do anel $\mathbb{Q}$ dos números racionais. O número 1 é a unidade de ambos.

- $L$ não possui unidade, mesmo $A$ sendo um anel com unidade. Por exemplo, $2\mathbb{Z}$ como subanel de $\mathbb{Z}$.

- $L$ e $A$ são anéis com unidade, mas as unidades são diferentes. Deixamos como exercício a verificação de que isso acontece, por exemplo, com o anel $M_2(\mathbb{R})$ e o subanel $L$ constituído pelas matrizes do tipo

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

Enquanto a unidade de $M_2(\mathbb{R})$ é $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, a de $L$ é $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ (verificar).

- Nem $L$ nem $A$ possuem unidade. Isso ocorre, por exemplo, com $4\mathbb{Z} = \{0, \pm 4, \pm 8, ...\}$ como subanel de $2\mathbb{Z} = \{0, \pm 2, \pm 4, ...\}$.

• $A$ não é um anel com unidade, mas $L$ possui unidade. É o caso, por exemplo, do anel $A = 2\mathbb{Z} \times \mathbb{Z}$ (produto direto), que nao possui unidade, e de $L = \{0\} \times \mathbb{Z}$, que é subanel de $A$ e cuja unidade é o par $(0, 1)$. (Sugerimos, como exercício, a verificaçao desses fatos.)

**Definição 7:** Sejam $A$ um anel e $L$ um subanel de $A$, ambos com unidade. Se $1_A = 1_B$, diz se que $L$ é um *subanel unitário* de $A$.

*Exemplo 13:* Se $L$ é um subanel do anel $\mathbb{R}$ dos número reais e $L$ possui unidade, então essa unidade é a mesma de $\mathbb{R}$, ou seja, é o número real 1.

Seja $1_L$ a unidade de $L$. Então,

$$1_L \cdot 1_L \overset{*}{=} 1_L \overset{**}{=} 1 \cdot 1_L$$

Cancelando-se $1_L$ na igualdade $1_L \cdot 1_L = 1 \cdot 1_L$, obtém-se $1_L = 1$.

Notar que na passagem assinalada com * usamos o fato de que $1_L \in L$ e que $1_L$ é a unidade de $L$ e na passagem assinalada com **, que $1_L \in \mathbb{R}$ (pois $L \subset \mathbb{R}$) e 1 é a unidade de $\mathbb{R}$. O estudante deverá notar que o raciocínio usado neste caso para $\mathbb{R}$ pode ser empregado para $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{C}$.

## 3.3 Anéis comutativos com unidade

**Definição 8:** Um anel cuja multiplicação é comutativa e que possui unidade chama-se *anel comutativo com unidade*.

*Exemplo 14:* Os anéis numéricos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

*Exemplo 15:* Se $A$ é um anel comutativo com unidade, o mesmo se pode dizer de $A^X$, qualquer que seja o conjunto $X \neq \varnothing$. (Ver exemplos 8 e 12.)

## 3.4 Anéis de integridade

Consideremos o anel dos inteiros $\mathbb{Z}$ e o anel $\mathbb{Z}^{\mathbb{Z}}$ das funções de $\mathbb{Z}$ em $\mathbb{Z}$. Embora ambos, como já vimos, sejam anéis comutativos com unidade, eles diferem num ponto muito importante. Isso porque, enquanto no primeiro vale a *lei do anulamento do produto*, ou seja:

"Se $a, b \in \mathbb{Z}$ e $ab = 0$, então $a = 0$ ou $b = 0$",

no segundo isso não acontece. De fato, consideremos as funções $f, g: \mathbb{Z} \to \mathbb{Z}$ definidas da seguinte maneira:

$f(0) = 1$ e $f(x) = 0$, sempre que $x \neq 0$;

$g(0) = 0$ e $g(x) = 1$, sempre que $x \neq 0$

Pela própria maneira como foram definidas, $f$ e $g$ são diferentes do *zero* do anel que e a função constante 0). Não obstante, $fg$ é o *zero* do anel, pois.

$$(fg)(0) = f(0)g(0) \quad 1 \cdot 0 \quad 0$$

e se $x \neq 0$:

$$(fg)(x) \quad f(x)g(x) = 0 \cdot 1 \quad 0$$

Portanto, no anel $\mathbb{Z}^{\mathbb{Z}}$ não se verifica a lei do anulamento do produto.

Essas duas possibilidades abrem espaço para a definição que segue.

**Definição 9:** Seja $A$ um anel comutativo com unidade. Se para esse anel vale a lei do anulamento do produto, ou seja, se uma igualdade do tipo

$$ab = 0_A$$

em que $a, b \in A$, só for possível para

$$a = 0_A \text{ ou } b = 0_A$$

então se diz que $A$ é um *anel de integridade* ou *domínio*. A forma contrapositiva dessa condição é a seguinte: Se $a \neq 0$ e $b \neq 0$, então $ab \neq 0$.

*Exemplo 16:* Todos os anéis numéricos, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, são anéis de integridade.

*Exemplo 17:* Consideremos o anel de integridade $\mathbb{Z}$ e um conjunto unitário $X = \{a\}$ e mostremos que $A = \mathbb{Z}^X$ é um anel de integridade. Que se trata de um anel comutativo com unidade, já vimos. Ademais, como os elementos de $A$ são as aplicações $f_n: X \to \mathbb{Z}$, definidas por $f_n(a) = n \, (n \in \mathbb{Z})$, então o zero desse anel é a aplicação $f_0$. Como $(f_r \cdot f_s)(a) = f_r(a)f_s(a) = rs = f_{rs}(a)$, então $f_r \cdot f_s = f_{rs}$. Assim, se $f_r \neq f_0$ e $f_s \neq f_0$, ou seja, $r \neq 0$ e $s \neq 0$, então $f_{rs} \neq 0$, uma vez que $rs \neq 0$.

No entanto, se $X$ possuir mais do que um elemento, então $A = \mathbb{Z}^X$ não é um anel de integridade. Sugerimos ao estudante provar esse fato. Para mostrar que não vale a lei do anulamento do produto em $A$, o raciocínio é o mesmo usado para o anel $\mathbb{Z}^{\mathbb{Z}}$.

Consideremos um anel comutativo $A$ em que não se verifica a lei do anulamento do produto. Isso significa que no anel há pelo menos um par de elementos $a$, $b \neq 0_A$ (eventualmente esses elementos são iguais) tais que $ab = 0_A$. Quando isso se verifica, diz-se que $a$ e $b$ são *divisores próprios do zero* do anel. Portanto, um anel de integridade pode ser definido como um anel comutativo com unidade que não possui divisores próprios do zero. Ou, ainda, como um anel comutativo com unidade cujo conjunto dos elementos diferentes do zero é fechado para a multiplicação.

*Exemplo 18:* Se $m > 1$ é um inteiro composto, então sempre há divisores próprios do zero no anel $\mathbb{Z}_m$. De fato, neste caso podem-se encontrar inteiros $a$ e $b$ tais que $0 < a, b < m$ e $m \mid ab$. Portanto, $a, b \in \mathbb{Z}_m$, $a, b \neq 0$ e $a \cdot b = ab = m = 0$. No anel $\mathbb{Z}_4$, por exemplo, o único divisor próprio do zero é o $\overline{2}$ (observar que $\overline{2} \cdot \overline{2} = \overline{4} = 0$).

**Proposição 3:** Um anel de classes de restos $\mathbb{Z}_m$ é anel de integridade se, e somente se, $m$ é um número primo.

$(\to)$ Se $m$ fosse composto, então $\mathbb{Z}_m$ possuiria divisores próprios do zero, como já se mostrou no exemplo 18. Mas isso contraria a hipótese.

$(\leftarrow)$ Como já sabemos, $\mathbb{Z}_m$ é um anel comutativo com unidade, qualquer que seja $m > 1$. Suponhamos, com a hipótese feita, que $a \cdot b = ab = 0$, para algum par

de elementos $\bar{a}, \bar{b} \in \mathbb{Z}_m$. Daí, $ab = mq$ (com $q \in \mathbb{Z}$) e, portanto, $m \mid ab$. Mas, como $m$ é primo, por hipótese, então $m \mid a$ ou $m \mid b$. Mas essas relações, em termos de classes de equivalência, se traduzem por $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Ou seja, se $m$ é primo, então $\mathbb{Z}_m$ não possui divisores próprios do zero e conseqüentemente é um anel de integridade. #

**Proposição 4:** Seja $A$ um anel comutativo com unidade $A$. Então $A$ é um anel de integridade se, e somente se, todo elemento não nulo de $A$ é regular para a multiplicação. (Lembremos que ser *regular* significa obedecer à lei do cancelamento.)

*Demonstração:*

($\rightarrow$) Sejam $a, b, c \in A$, $a \neq 0$, e suponhamos $ab = ac$. Daí, $ab - ac = 0$ e, portanto, $a(b - c) = 0$. Como $A$, por ser um anel de integridade, não possui divisores próprios do zero, então $b - c = 0$, e, portanto, $b = c$. Isso mostra que $a$ é regular para a multiplicação.

($\leftarrow$) Temos de provar apenas que não há divisores próprios do zero em $A$. Para isso, indiquemos por $a$ um suposto divisor próprio do zero de $A$. Então $a \neq 0$ e $ab = 0$ para algum $b \in A$, $b \neq 0$. Mas, como $0 = a \cdot 0$, então $ab = a \cdot 0$. A hipótese de que $a$ é regular, e que, portanto, pode ser cancelado nessa igualdade, nos obriga a concluir que $b = 0$, o que não é possível. De onde, efetivamente não há divisores próprios do zero em $A$. #

## 3.5 Corpos

Lembremos primeiro que a unidade e o zero de um anel com unidade são elementos diferentes (definição 5). Portanto, num anel com unidade, as equações $0 \cdot x = 1$ e $x \cdot 0 = 1$ não têm solução. Ou seja, o zero de um anel com unidade, qualquer que seja ele, não tem simétrico multiplicativo (inverso). Por outro lado, como $1 \cdot 1 = 1$ e $(-1)(-1) = 1$, a unidade de um anel com unidade e seu oposto sempre têm simétrico multiplicativo. No que segue, adotaremos a notação $U(A)$ para indicar os elementos de um anel que têm inverso, elementos esses que serão chamados de *inversíveis*. Como vimos, $U(A)$ nunca é vazio, mas também nunca inclui o zero.

Ocorre que há certos anéis comutativos com unidade em que só o zero não é inversível. É o caso, por exemplo, dos anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. E anéis em que, além do zero, há outros elementos não inversíveis, como, por exemplo, o anel $\mathbb{Z}$ dos números inteiros. Na verdade, $U(\mathbb{Z}) = \{-1, +1\}$. A definição que segue diz respeito à primeira dessas possibilidades.

**Definição 10:** Seja $K$ um anel comutativo com unidade. Se $U(K) = K^* = K - \{0\}$, então $K$ recebe o nome de *corpo*.

*Exemplo 19:* Os anéis numéricos, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, são corpos.

*Contra exemplo 3:* O anel $A = \mathbb{R}^{\mathbb{R}}$ das funções reais de uma variável real não é um corpo. Para provar esse fato, lembremos que a unidade desse anel é a função

$u: \mathbb{R} \to \mathbb{R}$, definida por $u(x) = 1$, qualquer que seja $x \in \mathbb{R}$. Isso posto, consideremos a função $f: \mathbb{R} \to \mathbb{R}$ assim definida: $f(0) = 0$ e $f(x) = 5$, sempre que $x \neq 0$. Por não ser a função constante 0, $f$ não é o zero do anel $\mathbb{R}^{\mathbb{R}}$. E como, qualquer que seja a função $g: \mathbb{R} \to \mathbb{R}$,

$$(fg)(0) = f(0)g(0) = 0 \cdot g(0) = 0$$

então $fg \neq u$. Ou seja, $f$ não é inversível.

**Proposição 5:** Todo corpo é um anel de integridade.

*Demonstração:* Temos de provar apenas que num corpo vale a lei do anulamento do produto. Para isso, sejam $K$ um corpo e $a, b \in K$ tais que $ab = 0$. Suponhamos, por exemplo, que $a \neq 0$ e que, portanto, $a$ é inversível. Multiplicando-se os dois membros da igualdade $ab = 0$ por $a^{-1}$:

$$a^{-1}(ab) = a^{-1} \cdot 0 = 0$$

Porém, como $a^{-1}(ab) = b$, então $b = 0$.

Analogamente se demonstra que, se $b \neq 0$, então $a = 0$. Então um produto de dois fatores de $K$ não pode ser nulo sem que um deles o seja, o que demonstra que $K$ é um anel de integridade. #

A recíproca dessa proposição não é verdadeira. De fato, o anel $\mathbb{Z}$, por exemplo, é um anel de integridade mas não é um corpo, pois $U(\mathbb{Z}) = \{-1, +1\}$. Mas numa situação muito especial essa recíproca vale, como veremos a seguir: quando o anel de integridade é finito. Para a demonstração desse fato usaremos o seguinte resultado da teoria dos conjuntos: se um conjunto $A$ é finito e $f: A \to A$ é uma aplicação injetora, então $f$ é sobrejetora e, portanto, $Im(f) = A$. Diga-se de passagem que, embora esse resultado seja bastante intuitivo, sua demonstração não é nada imediata.

**Proposição 6:** Todo anel de integridade finito é um corpo.

*Demonstração:* Seja $A$ um anel de integridade formado de $n$ elementos, digamos, $A = \{a_1, a_2, ..., a_n\}$. O artifício da demonstração, como já adiantamos, é descobrir uma conveniente aplicação injetora de $A$ em $A$. E, para isso, usaremos o fato de que todo elemento de $A - \{0\}$ é regular para a multiplicação. Seja $a$ um desses elementos e consideremos $f: A \to A$ assim definida: $f(a_i) = aa_i$ $(i = 1, 2, ..., n)$.

Se $f(a_i) = f(a_j)$, então $aa_i = aa_j$ e daí, cancelando-se $a$ (o que é possível, pois $a \neq 0$ e $A$ é um anel de integridade), $a_i = a_j$. Isso mostra que $f$ é injetora e, portanto, como já observamos, que $f$ é uma bijeção. Portanto:

$$Im(f) = \{aa_1, aa_2, ..., aa_n\} = A$$

Assim, a unidade do anel, que é um dos elementos $a_i$, pode ser escrita como

$$1 = aa_r$$

para algum $r$, $1 \leq r \leq n$. Ou seja, $a$ é inversível. Se todo elemento de $A$, diferente do zero, é inversível, então $A$ é um corpo, como queríamos demonstrar. #

*Exemplo 20:* Se $p$ é um número primo positivo, então $\mathbb{Z}_p$ é um corpo. De fato como já foi demonstrado (proposição 3), neste caso $\mathbb{Z}_p$ é um anel de integridade E como é finito, a proposição 6 nos assegura que $\mathbb{Z}_p$ é um corpo.

Segue uma maneira equivalente, às vezes mais conveniente, de definir *corpo*.

**Definição 10':** Um objeto matemático constituído de um conjunto não vazio $K$, uma adição e uma multiplicação sobre $K$ recebe o nome de *corpo* (i) se $K$ é um grupo abeliano no que se refere à adição; (ii) se 0 indica o elemento neutro da adição, $K^* = K - \{0\}$ é um grupo abeliano no que se refere à multiplicação, (iii) se a multiplicação é distributiva em relação à adição.

Na seqüência, segue a *justificação* da equivalência entre as definições 10 e 10'.

(Definição 10) → (Definição 10')

Por hipótese, $K$ é um corpo, conforme a definição 10. Por conseguinte, $(K, +)$ é um grupo abeliano. Por outro lado, como $K$ é um anel de integridade (proposição 5), então $K^* = K - \{0_K\}$ é fechado para a multiplicação. Além disso, $1_K \neq 0_K$ (definição) e, portanto, $1_K \in K^*$. E também, se $a \in K^*$, então $a^{-1} \in K^*$, pois $aa^{-1} = 1_K$. Quanto à associatividade e à comutatividade da multiplicação, como valem em $K$ valem também em qualquer parte fechada de $K$, em particular em $K^*$. Portanto, $(K^*, \cdot)$ é um grupo abeliano. A distributividade da multiplicação em relação à adição vale por hipótese.

(Definição 10') → (Definição 10)

Neste caso, cumpre mostrar que a associatividade e a comutatividade da multiplicação, que, por hipótese, valem em $K^*$, podem ser estendidas para $K$. Acontece que a demonstração da propriedade 2.2 (b), desta seção, poderia ser reproduzida aqui, textualmente, com as hipóteses com que contamos. Ou seja, com essas hipóteses demonstra-se que $a \cdot 0_K = 0_K \cdot a = 0_K$, qualquer que seja $a \in K$. Assim, por exemplo, dados $a, b \in K$, se um dos fatores é igual a $0_K$, então $ab = 0_K = ba$ e, portanto, a comutatividade da multiplicação, que vale em $K^*$, por hipótese, vale também em $K$. Coisa análoga acontece com a associatividade da multiplicação: o fato de valer em $K^*$ implica que vale em $K$. Quanto à unidade, é o elemento neutro do grupo $K^*$ (por quê?). #

**Definição 11** (subcorpo): Seja $(K, +, \cdot)$ um corpo. Um subconjunto não vazio $L \subset K$ é chamado *subcorpo* de $K$ se é fechado para a adição e a multiplicação de $K$ e se $L$ também tem uma estrutura de corpo (claro, para as operações de $K$, restritas aos elementos de $L$).

*Exemplo 21:* $\mathbb{Q}$ é subcorpo de $\mathbb{R}$ que, por sua vez, é subcorpo de $\mathbb{C}$

**Proposição 7:** Sejam $K$ um corpo e $L$ um subconjunto não vazio de $K$. Para que $L$ seja um subcorpo de $K$ é necessário e suficiente que: (i) $0, 1 \in L$, (ii) se $x, y \in L$, então $x - y \in L$; (iii) se $x, y \in L$ e $y \neq 0$, então $xy^{-1} \in L$.

*Demonstração:* Por brevidade, demonstraremos apenas a condição suficiente Primeiro, observemos que da hipótese decorre diretamente que $L$ é um subgrupo do

grupo aditivo $K$. Além disso, se $x, y \in L^*$, então $x, y \in L$ e $y \neq 0$ e, daí, $xy^{-1} \in L$, por hipótese. Mas, como $x, y^{-1} \neq 0$, e estamos num corpo, então $xy^{-1} \in L^*$. Logo, $L^*$ é um subgrupo do grupo multiplicativo $K^*$. Que a adição e a multiplicação de $K$, quando restritas a $L$, são operações sobre esse conjunto decorre dessas conclusões e de que $x \cdot 0 = 0 \cdot x = 0$, qualquer que seja $x \in L$. Ademais, como a distributividade da multiplicação em relação à adição, por valer em $K$, vale também em $L$, a definição 10' garante que $L$ tem estrutura de corpo para as restrições das operações de $K$ a seus elementos. De onde, $L$ é subcorpo de $K$. #

*Exemplo 22:* Provar que $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é um subcorpo do corpo $\mathbb{R}$ dos números reais.

(i) $0 = 0 + 0 \cdot \sqrt{2}$ e $1 = 1 + 0 \cdot \sqrt{2}$; logo, $0, 1 \in L$.

(ii) Se $x, y \in L$, então esses elementos podem ser postos assim: $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ $(a, b, c, d \in \mathbb{Q})$. Logo, $x - y = (a - c) + (b - d)\sqrt{2}$. Como $(a - c)$, $(b - d) \in \mathbb{Q}$, então $x - y \in L$.

(iii) Se $x, y \in L$ e $y \neq 0$, então esses elementos podem ser representados assim: $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ $(a, b, c, d \in \mathbb{Q}, c \neq 0$ ou $d \neq 0)$. Então:

$$xy^{-1} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} =$$

$$= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}$$

Como $c^2 - 2d^2 \neq 0$, pois, caso contrário, $c/d = \sqrt{2}$, o que é impossível, já que $c, d \in \mathbb{Q}$, então $\dfrac{ac - 2bd}{c^2 - 2d^2}$ e $\dfrac{bc - ad}{c^2 - 2d^2}$ são números racionais e, portanto, $xy^{-1} \in L$.

## Exercícios

**1.** Prove que o conjunto $\mathbb{Z}$ dotado da lei usual de adição e da mulplicação definida por $a \cdot b = 0$, para quaisquer $a$ e $b$ em $\mathbb{Z}$, é um anel.

**2.** Mostre que o conjunto $\mathbb{Q}$ dotado das leis de composição $\oplus$ e $\odot$ abaixo definidas é um anel.

$$a \oplus b = a + b - 1$$
$$a \odot b = a + b - ab$$

**3.** Consideramos as operações $*$ e $\Delta$ em $\mathbb{Q}$ definidas por:

$$x * y = x + y - 3 \quad \text{e} \quad x \Delta y = x + y - \frac{xy}{3}$$

Mostre que $(\mathbb{Q}, *, \Delta)$ é um anel comutativo com elemento unidade.

**4.** Seja $A$ um anel. Em $A \times A$ estão definidas as duas operações seguintes

$$(a, b) \top (c, d) = (a + c, b + d)$$
$$(a, b) * (c, d) = (ac, 0)$$

Prove que $A \times A$ é um anel.

**5.** Demonstre que $\mathbb{Z} \times \mathbb{Z}$ munido das operações $*$ e $\Delta$ abaixo definidas é um anel.

$$(a, b) * (c, d) = (a + c, b + d)$$
$$(a, b)\ \Delta\ (c, d) = (ac, ad + bc)$$

**6.** Consideremos em $\mathbb{Z} \times \mathbb{Z}$ as operações $+$ e $\cdot$ definidas por:

$$(a, b) + (c, d) = (a + c, b + d) \ \text{ e } \ (a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

Mostre que $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade.

**7.** Seja $p$ um número primo. Seja $A$ o subconjunto de $\mathbb{Q}$ formado pelos números $\dfrac{m}{n}$ tais que $n \neq 0$ e $p \nmid n$. Mostre que $A$ é um anel.

**8.** Sejam $S$, um conjunto, $A$ um anel e $f: S \to A$ uma aplicação bijetora. Para cada par $x, y \in S$, definimos:

$$x + y = f^{-1}(f(x) + f(y)) \ \text{ e } \ xy = f^{-1}(f(x)f(y))$$

Mostre que essa soma e esse produto definem uma estrutura de anel sobre $S$.

**9.** Seja $E$ um conjunto não vazio. Em $\mathcal{P}(E)$ considere as operações:

$$x\ \Delta\ y = (x \cup y) - (x \cap y) \ \text{ e } \ x \cdot y = x \cap y$$

Admitindo conhecidas as propriedades da reunião e da interseção de conjuntos, prove que $(\mathcal{P}(E), \Delta, \cdot)$ é um anel comutativo com unidade.

**10.** Consideremos as operações $*$ e $\Delta$ em $\mathbb{Z}$ definidas por:

$$x * y = x + ay - 2 \ \text{ e } \ x\ \Delta\ y = xy + bx + cy + d$$

em que $a, b, c, d$ são números inteiros dados.
Determine $a, b, c, d$ de modo que $(\mathbb{Z}, *, \Delta)$ seja um anel. Para os valores obtidos de $a, b, c, d$, $(\mathbb{Z}, *, \Delta)$ é um anel comutativo com unidade?

**11.** Seja $A$ um anel cujas duas leis de composição são iguais, isto é, $a + b = ab$, $\forall a, b \in A$. Mostre que $A = \{0\}$.

**12.** Seja $A$ um anel. Mostre que $a(b - c) = ab - ac$ e $(a - b)c = ac - bc$, quaisquer que sejam $a, b, c \in A$.

**13.** Seja $A$ um anel em que $x^2 = x$, para todo $x \in A$. Mostre que $-x = x$, $\forall x \in A$ e $A$ é comutativo.

*Sugestão:* Considere os produtos $(x + x)^2$ e $(x + y)^2$.

**14.** Seja $(A, +, \cdot)$ um anel com unidade. Mostre que a comutatividade da adição é consequência dos demais axiomas que compoem a definição de anel.
*Sugestão:* Prove que $(a + b) - (b + a) = 0$

**15.** Sendo $a$ e $b$ elementos de um anel comutativo $A$, mostre que
$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \ldots + \binom{n}{1}ab^{n-1} + b^n, \forall n \geq 0, n \in \mathbb{Z}$.

**16.** Construa as tábuas da adição e da multiplicação no anel $A = \{a, b\}$ com dois elementos distintos.

**17.** Construa as tábuas da adição e da multiplicação no anel $A = \{a, b, c\}$ com três elementos, todos distintos.

**18.** Sabe-se que $A = \{a, b, c, d\}$ e $(A, +, \cdot)$ é um anel em que os elementos neutros das operações $+$ e $\cdot$ são, respectivamente, $a$ e $b$. Conhecendo-se os compostos $b + b = a, c + c = a, cd = a$, construa as tábuas das duas operações.

**19.** Verifique se existe um anel $A = \{a, b, c, d\}$ tal que $(A, +)$ é isomorfo como grupo ao $\mathbb{Z}_4$ e $x^2 = x, \forall x \in A$.

**20.** Determine quais dos seguintes subconjuntos de $\mathbb{Q}$ são subanéis:

a) $\mathbb{Z}$

b) $B = \{x \in \mathbb{Q} \mid x \notin \mathbb{Z}\}$

c) $C = \left\{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, 2 \mid b\right\}$

d) $D = \left\{\frac{a}{2^n} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ e } n \in \mathbb{Z}\right\}$

**21.** Verique se são subanéis:

a) $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ do anel $\mathbb{R}$;

b) $\mathbb{Z}$ do anel do exercício 2;

c) $2\mathbb{Z} \times 2\mathbb{Z}$ do exercício 5.

**22.** Quais dos conjuntos abaixo são subanéis de $M_2(\mathbb{R})$?

$L_1 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$

$L_2 = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$

$L_3 = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$

$L_4 = \left\{\begin{pmatrix} 0 & a \\ c & b \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$

**23.** Mostre que $\mathbb{Q}^{\mathbb{Q}}$ (conjunto das funções de $\mathbb{Q}$ em $\mathbb{Q}$) é um subanel de $\mathbb{R}^{\mathbb{R}}$ (anel em relação à adição e à multiplicação de funções).

**24.** Se $B$ e $C$ são subanéis de $A$, então $B \cap C$ é subanel de $A$. Prove.

**25.** Ache todos os subanéis do anel $\mathbb{Z}_6$.
*Sugestão:* Determine todos os subgrupos de $(\mathbb{Z}_6, +)$ e verifique quais são fecha dos para a multiplicação.

**26.** Resolva a equação $3x + 2 = 6x + 7$ no anel $\mathbb{Z}_8$.

**27.** Determine $x$ em $\mathbb{Z}_5$ tal que $3x + 1 = 2$.

**28.** Resolva o sistema de equações: $\begin{cases} 3x + 2y = 1 \\ 4x + 6y = 2 \end{cases}$ no anel $\mathbb{Z}_7$

**29.** Detemine $x, y \in \mathbb{Z}_{12}$, satisfazendo o sistema de equações:
$\begin{cases} 6x + 5y = 7 \\ 3x + y = 2 \end{cases}$

**30.** Chama-se comutador de dois elementos $x$ e $y$ de um anel $A$ ao elemento $f(x, y) = xy - yx$. Mostre que:

a) $x$ e $y$ comutam se, e somente se, $f(x, y) = 0$;
b) $f(x, x) = 0, \forall x \in A$;
c) $f(x, y) = -f(y, x), \forall x, y \in A$;
d) $f(x, f(y, z)) + f(y, f(z, x)) + f(z, f(x, y)) = 0$ (Identidade de Jacobi).

**31.** Determine o conjunto dos elementos regulares para a multiplicação e o conjunto dos elementos inversíveis de cada um dos seguintes anéis:

a) $\mathbb{Z}$
b) $\mathbb{Q}$
c) $\mathbb{Z} \times \mathbb{Z}$ (produto direto)
d) $\mathbb{Z}_3$
e) $\mathbb{Z}_4$
f) $\mathbb{Z}_{14}$
g) $M_2(\mathbb{R})$
h) $\mathbb{Z}_2 \times \mathbb{Z}_3$

**32.** Que anéis do exercício 31 são de integridade? E que anéis são corpos?

**33** Determine todos os divisores próprios de zero, todos os elementos regulares para a multiplicaçao e todos os elementos inversíveis do anel $\mathbb{Z}_{24}$.

**34.** Ache os elementos inversíveis dos seguintes anéis:

a) $(\mathbb{Q}, \oplus, \odot)$, em que $a \oplus b = a + b - 1$ e $a \odot b = a + b - ab$

$(\mathbb{Q}, \oplus, \odot)$ é um corpo?

b) $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$, em que $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (ac, ad + bc)$

**35.** Determine os divisores próprios de zero do anel $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ do exercício anterior.

**36.** Dê exemplo de um anel com unidade em que só a unidade é inversível.

**37.** a) Quais são os elementos inversíveis do anel $\mathbb{Z}_{18}$?

b) Resolva em $\mathbb{Z}_{18}$ o sistema:

$$\begin{cases} \bar{5}x + \bar{2}y = \bar{1} \\ x + \overline{11}y = \bar{7} \end{cases}$$

**38.** Quais dos conjuntos abaixo são anéis de integridade? Suponha que a adição e a multiplicação são as usuais.

a) $A = \{2x + 1 \mid x \in \mathbb{Z}\}$

b) $B = \{2x \mid x \in \mathbb{Z}\}$

c) $C = \{x\sqrt{2} \mid x \in \mathbb{Q}\}$

d) $D = \{x + y\sqrt{3} \mid x, y \in \mathbb{Z}\}$

e) $E = \{x + y\sqrt{3} \mid x, y \in \mathbb{Q}\}$

f) $F = \{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} \mid a, b, c, d \in \mathbb{Z}\}$

**39.** Mostre que $A = \{(z_1, z_2, -z_2, z_1) \mid z_1, z_2 \in \mathbb{C}\}$, com adição e a multiplicação definidas por

$$(a, b, c, d) + (e, f, g, h) = (a + e, b + f, c + g, d + h)$$
$$(a, b, c, d) \cdot (e, f, g, h) = (ae + bg, af + bh, ce + dg, cf + dh)$$

é um anel comutativo com unidade.

**40.** Mostre que $A = \{(a, b, -b, a) \mid a, b \in \mathbb{Q}\}$, com adição e a multiplicação definidas por

$$(a, b, c, d) + (e, f, g, h) = (a + e, b + f, c + g, d + h)$$
$$(a, b, c, d) \cdot (e, f, g, h) = (ae + bg, af + bh, ce + dg, cf + dh)$$

é um corpo.

**41.** Considere $A = \{(a_1, a_2, a_3, a_4) \mid a_i \in \mathbb{R}\}$, com adição e a multiplicação definidas respectivamente por:

$$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4)$$
$$(a_1, a_2, a_3, a_4)(b_1, b_2, b_3, b_4) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3, a_4 \cdot b_4)$$

Sabendo que $A$ é um anel comutativo com unidade, mostre que $A$ nao é anel de integridade.

**42.** Um elemento $a$ de um anel $A$ se diz idempotente se $a^2 = a$ e nilpotente se existe $n \in \mathbb{N}^*$, de modo que $a^n = 0$. Mostre que o único elemento não nulo e idempotente de um anel de integridade é a unidade e que o zero e o único elemento nilpotente de um anel de integridade.

**43.** Se $E$ é um conjunto não vazio, mostre que no anel $A = \mathcal{P}(E)$ todos os elementos sao idempotentes (Ver exercício 9.)

**44.** Ache o conjunto dos elementos nilpotentes dos seguintes anels, $\mathbb{Z}$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ e $\mathbb{R}^{\mathbb{R}}$.

**45.** Mostre que o conjunto dos elementos nilpotentes de um anel comutativo $A$ é um subanel de $A$.

**46.** Prove detalhadamente o seguinte: se $a \in A$ (anel de integridade) e $a^2 = 1$, então $a = 1$ ou $a = -1$.

**47.** Mostre que se $A$ é um anel de integridade, $x \in A$ e $x^2 = x$, então $x = 0$ ou $x = 1$.

**48.** Seja $A$ um anel com unidade tal que $x^2 = x$, $\forall x \in A$. Mostre que $A$ é um anel de integridade se, e somente se, $A = \{0, 1\}$.

**49.** Verdadeiro ou falso: se $A$ é um anel de integridade e $L$ é um subanel de $A$, então $1_A = 1_L$. Justifique.

**50.** Seja $A$ um anel que possui um elemento $e$ tal que $e^2 = e$, e não é um divisor próprio de zero de $A$. Mostre que $e$ é a unidade de $A$.

**51.** Sejam $A$ e $B$ anéis com unidade. Ache os divisores próprios de zero de $A \times B$, bem como os elementos inversíveis desse anel. Pode $A \times B$ (produto direto) ser um corpo?

**52.** Seja $K$ o conjunto dos números do tipo $a + bi$, em que $a$ e $b$ são racionais e $i$ e a unidade imaginária. Mostre que $K$ é um corpo.
*Sugestao* Prove que $K$ é um subcorpo de $\mathbb{C}$.

**53.** Determine quais dos seguintes subconjuntos de $\mathbb{R}$ sao subcorpos:

a) $A = \{a + b\sqrt{2} \mid a \in \mathbb{Q} \text{ e } b \in \mathbb{Q}\}$

b) $B = \{a + b\sqrt[3]{2} \mid a \in \mathbb{Q} \text{ e } b \in \mathbb{Q}\}$

c) $C = \{a\sqrt{2} + b\sqrt{3} \mid a \in \mathbb{Q} \text{ e } b \in \mathbb{Q}\}$

d) $D = \{a + b\sqrt{2} \mid a \in \mathbb{Z} \text{ e } b \in \mathbb{Z}\}$

**54.** O subconjunto $M = \{0, 1\}$ de um corpo $K$ qualquer é subcorpo de $K$?

**55.** Se $B$ e $C$ são subcorpos de um corpo $A$, então $B \cap C$ é um subcorpo de $A$.

**56.** Verdadeiro ou falso: existem infinitos subcorpos de $\mathbb{R}$?
Dê uma justificativa razoável para a resposta.

**57.** Prove que o único subcorpo de $\mathbb{Q}$ é o próprio $\mathbb{Q}$.

**58.** Mostre que $(a + b)^p = a^p + b^p$, quaisquer que sejam $a$ e $b$ em $\mathbb{Z}_p$, com $p$ número primo.

### Exercícios complementares

**C1.** Seja $M$ um subconjunto não vazio de um anel $A$ e seja $C(M)$ o conjunto dos elementos de $A$ que comutam com todos os elementos de $M$. Mostre que $C(M)$ é um subanel de $A$.

**C2.** Seja $K = \{0, 1, a, b\}$ um corpo. Construa as tábuas da adição e da multiplicação desse corpo.
*Sugestão:* Comece com a tabua da multiplicação; depois mostre que $a + b = 1$, $1 + a = b$, etc.

**C3.** Prove que $\mathbb{Q}$ é o "menor" subcorpo de $\mathbb{R}$.
*Sugestao.* Prove que, se $K$ é subcorpo de $\mathbb{R}$, então $\mathbb{Q} \subset K$.

# V-2 HOMOMORFISMOS E ISOMORFISMOS DE ANÉIS

## 4. INTRODUÇÃO

Tal como no caso dos grupos, o papel dos isomorfismos de anéis, conceito central desta seção, é em essência o de separar os anéis em classes disjuntas, de maneira tal que as propriedades pertinentes à estrutura de anel deduzidas para um dos representantes de uma das classes possam ser estendidas para todos os outros anéis da mesma classe, apenas mudando-se convenientemente as notações (dos elementos e das operações). Ou, dito de outro modo, que um anel de uma dada classe possa substituir eventualmente, em tudo o que diga respeito à estrutura de anel, outro qualquer dessa classe, sempre que isso possa ser conveniente. Reflete bem essa situação imaginar os anéis de uma mesma classe como "cópias" uns dos outros.

Essa idéia pressupõe, de um lado, uma correspondência biunívoca entre todos os anéis da mesma classe. E, de outro, que essa correspondência preserve as operações envolvidas, no sentido da definição 12.

## 5. HOMOMORFISMOS DE ANÉIS

**Definição 12:** Dá-se o nome de *homomorfismo* de um anel $(A, +, \cdot)$ num anel $(B, +, \cdot)$ a toda aplicação $f: A \to B$ tal que, quaisquer que sejam $x, y \in A$:

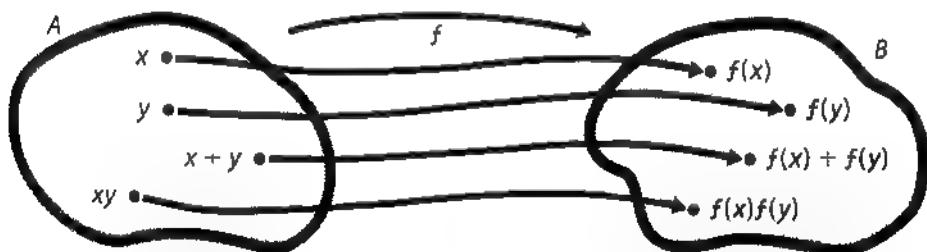
$$f(x + y) = f(x) + f(y)$$

e

$$f(xy) = f(x)f(y).$$

Nessas condições, para simplificar a linguagem, nos referiremos a $f: A \to B$ como um *homomorfismo de anéis*. Quando se tratar do mesmo anel, o que pressupõe $A = B$, a mesma adição e a mesma multiplicação em $A$, tanto como domínio como contradomínio, então $f$ será chamada de *homomorfismo* de $A$.

Se um homomorfismo é uma função injetora, então é chamado de *homomorfismo injetor*. E, se for uma função sobrejetora, de *homomorfismo sobrejetor*. O caso em que $f$ é bijetora corresponde ao conceito de *isomorfismo* e será estudado separadamente.

Convém observar ainda que, se $A$ e $B$ são anéis, então $(A, +)$ e $(B, +)$ são grupos e, portanto, um homomorfismo de anéis $f: A \to B$ também é um homomorfismo do grupo aditivo $A$ no grupo aditivo $B$.

*Exemplo 23:* Quaisquer que sejam os anéis $A$ e $B$, a aplicação $f: A \to B$, $f(x) = 0_B$ $(x \in A)$ é um homomorfismo de anéis, já que:

- $f(a + b) = 0_B = 0_B + 0_B = f(a) + f(b)$;
- $f(ab) = 0_B = 0_B \cdot 0_B = f(a)f(b)$.

*Exemplo 24:* Consideremos os anéis $A = \mathbb{Z}$ e $B = \mathbb{Z} \times \mathbb{Z}$ (produto direto) e a aplicação $f: A \to B$ assim definida: $f(n) = (n, 0)$. A aplicação $f$ é um homomorfismo, pois:

- $f(m + n) = (m + n, 0) = (m, 0) + (n, 0) = f(m) + f(n)$;
- $f(mn) = (mn, 0) = (m, 0)(n, 0) = f(m)f(n)$

*Exemplo 25.* Para cada inteiro $m > 1$, há um homomorfismo natural do anel $\mathbb{Z}$ no anel $\mathbb{Z}_m$ das classes de resto módulo $m$: a aplicação $p_m: \mathbb{Z} \to \mathbb{Z}_m$ definida por $p_m(r) = \overline{r}$, para cada $r \in \mathbb{Z}$. De fato, para quaisquer $r, s \in \mathbb{Z}$:

- $p_m(r + s) = \overline{r + s} = \overline{r} + \overline{s} = p_m(r) + p_m(s)$;
- $p_m(rs) = \overline{rs} = \overline{r}\,\overline{s} = p_m(r)p_m(s)$

$p_m$ é um homomorfismo sobrejetor, porque todo $y \in \mathbb{Z}_m$ é uma classe $y = \overline{r}$, que obviamente provém de $r \in \mathbb{Z}$ através de $p_m$.

*Exemplo 26:* Seja $A = \mathbb{Z}\left[\sqrt{2}\right] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ e consideremos $f: A \to A$ assim definida: $f\left(m + n\sqrt{2}\right) = m - n\sqrt{2}$ · $f$ é um homomorfismo de anéis, pois:

- $f\left(\left(m + n\sqrt{2}\right) + \left(r + s\sqrt{2}\right)\right) = f\left((m + r) + (n + s)\sqrt{2}\right) = (m + r) - (n + s)\sqrt{2}$

e também

$f\left(m + n\sqrt{2}\right) + f\left(r + s\sqrt{2}\right) = \left(m - n\sqrt{2}\right) + \left(r - s\sqrt{2}\right) = (m + r) - (n + s)\sqrt{2}$

- $f\left(\left(m + n\sqrt{2}\right)\left(r + s\sqrt{2}\right)\right) = f\left((mr + 2ns) + (ms + nr)\sqrt{2}\right) = (mr + 2ns) -$ $- (ms + nr)\sqrt{2}$

e também

$f\left(m + n\sqrt{2}\right)f\left(r + s\sqrt{2}\right) = \left(m - n\sqrt{2}\right)\left(r - s\sqrt{2}\right) = (mr + 2ns) - (ms + nr)\sqrt{2}$.

## 6. PROPOSIÇÕES SOBRE HOMOMORFISMOS DE ANÉIS

**Proposição 8:** Se $f: A \to B$ é um homomorfismo de anéis, então: (i) $f(0_A) = 0_B$; (ii) $f(-a) = -f(a)$; (iii) $f(a - b) = f(a) - f(b)$.

Essas propriedades decorrem do fato de que $f$ é um homomorfismo do grupo aditivo $A$ no grupo aditivo $B$. #

**Proposição 9:** Seja $f: A \to B$ um homomorfismo sobrejetor de anéis e suponhamos que $A$ possua unidade. Então: (i) $f(1_A)$ é a unidade de $B$ e, portanto, $B$ também é um anel com unidade; (ii) se $a \in A$ é inversível, então $f(a)$ também o é e $[f(a)]^{-1} = f(a^{-1})$.

*Demonstração:*

(i) Seja $b$ um elemento arbitrário de $B$. Como $f$ é sobrejetora, então $b = f(a)$, para algum $a \in A$. Portanto:

$$b \cdot f(1_A) = f(a)f(1_A) = f(a \cdot 1_A) = f(a) = b$$

Analogamente se mostra que $f(1_A) \cdot b = b$. Logo, $f(1_A)$ é a unidade de $B$.

(ii) Observemos que:

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$$

De modo análogo:

$$f(a^{-1})f(a) = f(a^{-1}a) = f(1_A) = 1_B$$

Portanto:

$$f(a^{-1}) = [f(a)]^{-1} \;\#$$

*Contra exemplo 4:* O homomorfismo $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ do exemplo 24 não é sobrejetor, pois $Im(f) = \{(n, 0) \mid n \in \mathbb{Z}\} \neq \mathbb{Z} \times \mathbb{Z}$. Neste caso, $f(1) = (1, 0) \neq (1, 1)$, ou seja, a imagem da unidade de $\mathbb{Z}$ (o número 1) não é a unidade de $\mathbb{Z} \times \mathbb{Z}$, que é o par $(1, 1)$.

**Proposição 10:** (i) Se $f: A \to B$ é um homomorfismo de anéis e $L$ é um subanel de $A$, então $f(L)$ é um subanel de $B$; (ii) se $f: M \to N$ é um homomorfismo de corpos, $f(1_m) \neq 0_n$ e $K$ é um subcorpo de $M$, então $f(K)$ é um subcorpo de $N$.

*Demonstração:*

Demonstraremos apenas (ii). A demonstração de (i) é análoga e fica proposta como exercício.

Sejam $c, d \in f(K)$. Então $c = f(a)$ e $d = f(b)$, para convenientes elementos $a$, $b \in K$. Logo:

$$c - d = f(a) - f(b) = f(a - b)$$

Como $a - b \in K$, pois $K$ é um subgrupo do grupo aditivo $M$, então $c - d \in f(K)$.

Além disso, se $d \neq 0$, então $b \neq 0$ e, portanto:

$$cd^{-1} = f(a)[f(b)]^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$$

Como $ab^{-1} \in K$, porque $K$ é subcorpo de $M$, então $cd^{-1} \in f(K)$. #

Em particular, com as condições da proposição, $Im(f)$ é um subanel (subcorpo) do contradomínio — naturalmente o próprio $B$ (ou $N$) se $f$ for sobrejetora.

*Exemplo 27:* Se $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ é o homomorfismo do exemplo 24, então $Im(f) = \{(n, 0) \mid n \in \mathbb{Z}\}$ é um subanel de $\mathbb{Z} \times \mathbb{Z}$.

**Proposição 11:** Sejam $f: A \to B$ e $g: B \to C$ homomorfismos de anéis. Então $g \circ f: A \to C$ também é um homomorfismo de anéis.

Deixamos a *demonstração* como exercício. Sugerimos ao estudante que tiver dúvidas reler a demonstração da proposição 5, capítulo IV. A argumentação é a mesma da demonstração citada — só que, obviamente, deverá ser usada para a adição e a multiplicação. #

## 7. NÚCLEO DE UM HOMOMORFISMO DE ANÉIS

**Definição 13:** Seja $f: A \to B$ um homomorfismo de anéis. Damos o nome de *núcleo de* f, e denotamos por $N(f)$ (usa-se também a notação $Ker(f)$), ao seguinte subconjunto de $A$:

$$N(f) = \{x \in A \mid f(x) = 0_B\}$$

Vale observar que, como $f(0_A) = 0_B$ (proposição 8), então $0_A \in N(f)$. Logo, pelo menos o zero de $A$ pertence ao núcleo de $f$.

*Exemplo 28:* O núcleo do homomorfismo do exemplo 23 é $A$, já que, devido à definição de $f$, todos os elementos de $A$ têm imagem igual a $0_B$.

*Exemplo 29:* Determinemos o nucleo do homomorfismo $p_m: \mathbb{Z} \to \mathbb{Z}_m$ do exemplo 25. Lembremos que $p_m$ é definido assim: $p_m(r) = \bar{r}$ $(r \in \mathbb{Z})$

Um inteiro $r \in N(p_m)$ se, e somente se, $\bar{r} = \bar{0}$;

se, e somente se, $r \equiv 0 \pmod{m}$;

se, e somente se, $r$ é múltiplo de $m$.

Portanto, $N(p_m) = \{0, \pm m, \pm 2m, ...\}$

*Exemplo 30:* Determinemos o núcleo do homomorfismo $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ do exemplo 24. Como o zero do anel $\mathbb{Z} \times \mathbb{Z}$ é o par $(0, 0)$, então um inteiro $n$ pertence a $N(f)$ se, e somente se, $f(n) = (n, 0) = (0, 0)$. Ou seja, se, e somente se, $n = 0$. Logo, $N(f) = \{0\}$.

*Exemplo 31:* Vamos encontrar agora o núcleo do homomorfismo $f$ do exemplo 26. Neste caso os anéis são $A = B = \mathbb{Z}[\sqrt{2}]$ e o zero de $B$ é o número 0. Então um número $a + b\sqrt{2}$ pertence a $N(f)$ se, e somente se, $f(a + b\sqrt{2}) = a - b\sqrt{2} = 0$. Mas isso implica que $a = b = 0$ e, portanto, $a + b\sqrt{2} = 0$. Logo, $N(f) = \{0\}$.

*Exemplo 32:* Consideremos $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida por $f(a, b) = a$. É fácil provar que $f$ é um homomorfismo de anéis (deixamos como exercício a verificação desse fato). Então um par $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ pertence a $N(f)$ se, e somente se, $f(a, b) = a =$ $= 0$. Portanto:

$$N(f) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid f(a, b) = a = 0\} = \{(0, b) \mid b \in \mathbb{Z}\}$$

Note-se que, neste caso, $N(f)$ é um conjunto infinito.

**Proposição 12:** Seja $f: A \to B$ um homomorfismo de anéis. Então: (i) $N(f)$ é um subanel de $A$; (ii) $f$ é injetor se, e somente se, $N(f) = \{0_A\}$.

*Demonstração:*

(i) Se $a, b \in N(f)$, então $f(a) = f(b) = 0_B$. Daí, $f(a - b) = f(a) - f(b) = 0_B$ e $f(ab) = f(a)f(b) = 0_B \cdot 0_B = 0_B$. Portanto, $a - b, ab \in N(f)$, o que prova que o núcleo de $f$ é um subanel de $A$.

(ii) Considerando-se que $A$ e $B$ são grupos aditivos e que $f$ é, em particular, um homomorfismo de grupos aditivos, então (devido à proposição 6, capítulo IV) $f$ é injetor se, e somente se, $N(f) = \{0_A\}$. #

## 8. ISOMORFISMO DE ANÉIS

Consideremos os anéis $\mathbb{Z}_6$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$ (produto direto), ambos constituídos de 6 elementos. À primeira vista, é difícil perceber algo em comum entre eles além da cardinalidade. afinal, os elementos e as operações de um e de outro têm natureza diferente. Na verdade, porém, pode-se mostrar que, enquanto anéis, eles "têm tudo" em comum.

Para mostrar isso, o primeiro passo é estabelecer uma correspondência biunívoca conveniente entre seus elementos. Essa tarefa não é fácil, mas uma boa saída é começar pela correspondência "mais natural" entre os elementos de um e de outro. Para isso, adotaremos a seguinte notação:

$\overset{6}{a}$ = classe de restos módulo 6 determinada por $a$;

$\overset{2}{a}$ = classe de restos módulo 2 determinada por $a$;

$\overset{3}{a}$ = classe de restos módulo 3 determinada por $a$.

Convenhamos que a correspondência "mais natural" de $\mathbb{Z}_6$ para $\mathbb{Z}_2 \times \mathbb{Z}_3$ é a "aplicação" $f$ (no exemplo 35 mostraremos que, de fato, $f$ é uma aplicação) assim definida:

$$\overset{6}{\bar{a}} \xrightarrow{f} (\overset{2}{\bar{a}}, \overset{3}{\bar{a}})$$

Numa tabela, mas, por simplicidade, sem o uso de traços sobre os elementos:

$f$

| $\mathbb{Z}_6$ | $\mathbb{Z}_2 \times \mathbb{Z}_3$ |
|---|---|
| 0 | (0, 0) |
| 1 | (1, 1) |
| 2 | (0, 2) |
| 3 | (1, 0) |
| 4 | (0, 1) |
| 5 | (1, 2) |

Observe-se que, por exemplo, o correspondente do 5 é o par (1, 2), porque o resto da divisão de 5 por 2 é 1 e por 3 é 2.

As tábuas do anel $\mathbb{Z}_6$ são fáceis de construir:

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| · | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

É uma questão de cálculos mostrar que, se substituirmos as entradas dessas tábuas pelos correspondentes elementos de $\mathbb{Z}_2 \times \mathbb{Z}_3$, obtêm-se como resultado exatamente as tábuas deste último anel. Ou seja, que a correspondência escolhida cumpre o esperado. No exemplo 35 provaremos formalmente essa afirmação. Aqui,

como ilustração, nos limitaremos a fazer duas verificações desse fato, uma para a tábua da adição e uma para a tábua da multiplicação.

Em $\mathbb{Z}_6$, por exemplo, $3 + 4 = 1$. Os correspondentes de 3 e 4 em $\mathbb{Z}_2 \times \mathbb{Z}_3$ são respectivamente $(1, 0)$, $(0, 1)$, cuja soma é $(1, 1)$, que é exatamente o correspondente de 1.

Também em $\mathbb{Z}_6$: $3 \cdot 4 = 0$. Multiplicando-se os correspondentes de 3 e 4, obtém-se:

$$(1, 0)(0, 1) = (0, 0)$$

que é o correspondente de 0.

De modo geral, se $a + b = c$ e $ab = d$ (em $\mathbb{Z}_6$), então $f(a) + f(b) = f(c)$ e $f(a)f(b) = f(d)$ (em $\mathbb{Z}_2 \times \mathbb{Z}_3$). Ou seja, $f$ preserva as operações, ou, falando mais formalmente, $f$ é um homomorfismo de anéis. Como é obviamente uma bijeção, então se trata de um exemplo de *isomorfismo de anéis*, conceito a ser definido a seguir.

**Definição 14:** Seja $f: A \to B$ um homomorfismo de anéis. Se $f$ for também uma uma bijeção, então será chamado de *isomorfismo* do anel $A$ no anel $B$. Neste caso, diz-se que $f$ é um *isomorfismo de anéis*.

Convém observar que um isomorfismo do anel $A$ no anel $B$ é, em particular, um isomorfismo do grupo aditivo $(A, +)$ no grupo aditivo $(B, +)$

*Exemplo 33* Se $A$ é um anel, então a aplicação idêntica $i_A: A \to A$, $i_A(x) = x$ é um isomorfismo de anéis, pois, além de ser bijetora, é também um homomorfismo, uma vez que.

- $i_A(a + b) = a + b = i_A(a) + i_A(b)$;
- $i_A(ab) = ab = i_A(a)i_A(b)$.

*Exemplo 34.* O homomorfismo $f: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, do exemplo 26, é um isomorfismo, pois é injetor, uma vez que $N(f) = \{0\}$, como mostramos no exemplo 31, e sobrejetor De fato, dado $y = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, basta tomar $x = m - n\sqrt{2} \in$ $\in \mathbb{Z}[\sqrt{2}]$ que:

$$f(x) = f(m - n\sqrt{2}) = m + n\sqrt{2} = y$$

*Exemplo 35:* A aplicação $f: \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ definida por $f(\overset{6}{\overline{a}}) = (\overset{2}{\overline{a}}, \overset{3}{\overline{a}})$, com a notação introduzida no início deste item, é um isomorfismo de anéis.

Mostraremos primeiro, e simultaneamente, que $f$ é, efetivamente, uma aplicação e que é injetora.

$\overset{6}{\overline{a}} = \overset{6}{\overline{b}}$ se, e somente se, $6 \mid (a - b)$;
se, e somente se, $2 \mid (a - b)$ e $3 \mid (a - b)$;
se, e somente se, $\overset{2}{\overline{a}} = \overset{2}{\overline{b}}$ e $\overset{3}{\overline{a}} = \overset{3}{\overline{b}}$;
se, e somente se, $(\overset{2}{\overline{a}}, \overset{3}{\overline{a}}) = (\overset{2}{\overline{b}}, \overset{3}{\overline{b}})$.

O fato de $f$ ser injetora e o domínio e o contra-domínio de $f$ terem a mesma cardinalidade ($= 6$) garantem que $f$ é sobrejetora.

Falta mostrar que $f$ preserva as operações, o que faremos apenas no que se refere à multiplicação:

$$f(\overset{6}{\bar{a}} \cdot \overset{6}{\bar{b}}) = f(\overset{6}{\overline{ab}}) = (\overset{2}{\overline{ab}}, \overset{3}{\overline{ab}}) = (\overset{2}{\bar{a}}\overset{2}{\bar{b}}, \overset{3}{\bar{a}}\overset{3}{\bar{b}}) = (\overset{2}{\bar{a}}, \overset{3}{\bar{a}})(\overset{2}{\bar{b}}, \overset{3}{\bar{b}}) = f(\overset{6}{\bar{a}}) \cdot f(\overset{6}{\bar{b}})$$

**Proposição 13:** Seja $f: A \to B$ um isomorfismo de anéis. Então $f^{-1}: B \to A$ também é um isomorfismo de anéis.

*Demonstração:* Sendo $f$ um isomorfismo do grupo aditivo $A$ no grupo aditivo $B$, então $f^{-1}$ é um isomorfismo do grupo aditivo $B$ no grupo aditivo $A$ (proposição 7, capítulo IV). Resta-nos provar que $f^{-1}$ preserva as multiplicações.

Sejam $c, d \in B$. Como $f$ é sobrejetora, $c = f(a)$ e $d = f(b)$, para convenientes elementos $a, b \in A$. Vale observar, de passagem, que essas igualdades equivalem respectivamente a $a = f^{-1}(c)$ e $b = f^{-1}(d)$. Isso posto:

$$f^{-1}(cd) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(c)f^{-1}(d) \ \#$$

Uma decorrência dessa proposição em termos de terminologia é que se $f: A \to B$ é um isomorfismo de anéis, então pode-se dizer que os anéis $A$ e $B$ são *isomorfos*. A relação estabelecida por um isomorfismo $f: A \to B$ será indicada por $A \approx B$ ou $B \approx A$. Dois anéis isomorfos diferem apenas pelos nomes de seus elementos e operações. Essencialmente são o mesmo anel e cada um deles pode ser considerado uma "cópia" do outro. Por exemplo, os anéis $\mathbb{Z}_6$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$ são isomorfos, como já mostramos. O anel $\mathbb{Z}_6$ pode ser considerado uma cópia mais favorável do anel $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Porem os anéis $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ não são isomorfos, como mostraremos a seguir.

*Contra exemplo 5:* Mostraremos que nenhuma aplicação de $\mathbb{Z}_4$ em $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um isomorfismo. Qualquer aplicação $f: \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ "candidata" a isomorfismo necessariamente levaria o zero no zero e a unidade na unidade. Isto é, $f(0) = (0, 0)$ e $f(1) = (1, 1)$. Então:

$$f(2) = f(1 + 1) = f(1) + f(1) = (1, 1) + (1, 1) = (1 + 1, 1 + 1) = (0, 0)$$

e

$$f(3) = f(1 + 2) = f(1) + f(2) = (1, 1) + (0, 0) = (1, 1)$$

Isso mostra que $f$ não é injetora, pois $f(0) = f(2)$ e $f(1) = f(3)$, nem sobrejetora, pois $Im(f) = \{(0, 0), (1, 1)\}$. Portanto, realmente não há nenhum isomorfismo de $\mathbb{Z}_4$ em $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Seja $f: A \to B$ um homomorfismo injetor de anéis (corpos). Se $L$ é um subanel (subcorpo) de $A$, então $f(L)$ é um subanel (subcorpo) de $B$, como já vimos (proposição 10). Então a aplicação $g: L \to f(L)$ definida por $g(x) = f(x)$, para qualquer $x \in L$, é um isomorfismo de anéis (corpos). De fato, $g$ é injetora, porque $f$ é injetora, é sobrejetora, porque $Im(g) = g(L) = f(L)$, e homomorfismo de anéis (corpos), porque $f$ o é. Portanto, se $f: A \to B$ é um homomorfismo injetor, todo subanel (subcorpo) $L$ de $A$ está retratado em $B$ por um subanel (subcorpo) que lhe é isomorfo: sua "cópia" $f(L)$.

*Exemplo 36:* Consideremos o homomorfismo $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ introduzido no exemplo 24 e assim definido: $f(n) = (n, 0)$. Como vimos (exemplo 30 e proposição 12), $f$ é um homomorfismo injetor. Lembremos que os subanéis de $\mathbb{Z}$ (todos) são os subconjuntos $n\mathbb{Z}$ ($n = 0, 1, 2, \ldots$). As "cópias" desses subanéis em $\mathbb{Z} \times \mathbb{Z}$ são os subanéis $n\mathbb{Z} \times \mathbb{Z}$ ($n = 0, 1, 2, \ldots$).

Mais: pode-se mostrar que os subconjuntos $n\mathbb{Z} \times \mathbb{Z}$ são os únicos subanéis de $\mathbb{Z} \times \mathbb{Z}$. De fato, sejam $M$ um subanel de $\mathbb{Z} \times \mathbb{Z}$ e $L$ o subconjunto de $\mathbb{Z}$ formado pelos primeiros termos dos elementos de $M$. Se $a_1, a_2 \in L$, então $(a_1, b_1), (a_2, b_2) \in M$, para convenientes $b_1, b_2 \in \mathbb{Z}$. Daí, $(a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \in M$ e, portanto, $a_1 - a_2 \in L$. Então $L$ é um subgrupo do grupo aditivo $\mathbb{Z}$ e, por isso, $L = n\mathbb{Z}$, para um conveniente $n \in \mathbb{Z}$. De onde $M = n\mathbb{Z} \times \mathbb{Z}$.

## Exercícios

**59.** Verifique se a função $f: A \to B$ é ou não é um homomorfismo do anel $A$ no anel $B$ nos seguintes casos:

a) $A = \mathbb{Z}, B = \mathbb{Z}, f(x) = x + 1$
b) $A = \mathbb{Z}, B = \mathbb{Z}, f(x) = 2x$
c) $A = \mathbb{Z}, B = \mathbb{Z} \times \mathbb{Z}, f(x) = (0, x)$
d) $A = \mathbb{Z} \times \mathbb{Z}, B = \mathbb{Z}, f(x, y) = x$
e) $A = \mathbb{Z} \times \mathbb{Z} = B, f(x, y) = (y, x)$
f) $A = \mathbb{Z}, B = \mathbb{Z}_n, f(x) = x$
g) $A = B = \mathbb{C}$ (corpo dos complexos) e $f(a + bi) = a - bi$

**60.** Determine os núcleos dos homomorfismos do exercício anterior.

**61.** Considere os anéis $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ (produto direto). Verifique se são homomorfismos e determine o núcleo.

a) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dado por $f(x, y) = (0, y)$
b) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dado por $f(x, y) = y$
c) $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dado por $f(x) = (2x, 0)$
d) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dado por $f(x, y) = (-y, -x)$
e) $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dado por $f(x) = (0, x)$

**62.** Sabendo que $\mathbb{Z} \times \mathbb{Z}$ munido das operações de adição e multiplicação assim definidas:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac, 0)$$

é um anel, mostre que a aplicação $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que $f(a, b) = a$ é um homomorfismo sobrejetor.

**63.** Sabe-se que $\mathbb{Z} \times \mathbb{Z}$ munido das operações de adição e multiplicação assim definidas:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac, ad + bc)$$

é um anel. Mostre que a aplicação $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que $f(a, b) = a$ é um homomorfismo de anéis.

**64.** Sabe-se que $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ é um anel quando a adição e a multiplicação são assim definidas:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

Mostre que a aplicação $f: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ tal que $f(a) = (a, 0)$ é um homomorfismo de $\mathbb{Z}$ em $\mathbb{Z} \times \mathbb{Z}$.

**65.** Dê um exemplo de anéis $A$ e $B$ e um homomorfismo $f: A \to B$ tal que $f(1_A) \neq 1_B$.

**66.** Mostre que $f: \mathbb{C} \to M_2(\mathbb{R})$ dada por $f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $\forall a, b \in \mathbb{R}$, é um homomorfismo injetor de anéis.

**Resolução**

Tomemos $z_1 = a + bi$ e $z_2 = c + di$ em $\mathbb{C}$.

Temos:

$$f(z_1 + z_2) = f((a + c) + (b + d)i) = \begin{pmatrix} a + c & -(b + d) \\ b + d & a + c \end{pmatrix} = \begin{pmatrix} a + c & -b - d \\ b + d & a + c \end{pmatrix} =$$
$$= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = f(z_1) + f(z_2)$$

$$f(z_1 \cdot z_2) = f((ac - bd) + (ad + bc)i) = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix} =$$
$$= \begin{pmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = f(z_1) \cdot f(z_2)$$

Observemos que $f$ é injetora, pois:

$$f(z_1) = f(z_2) \Rightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \Rightarrow \begin{cases} a = c \\ b = d \end{cases} \Rightarrow z_1 = z_2$$

■

**67.** Sejam os anéis $A = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$ e $B = M_2(\mathbb{Q})$.

a) Mostre que $f: A \to B$ dada por $f(a + b\sqrt{-2}) = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix}$ é um homomorfismo.

b) $f$ é um isomorfismo?

**68.** Considere os seguintes anéis $(\mathbb{R}, +, \cdot)$ e $(\mathbb{R}, \oplus, \odot)$, sendo $a \oplus b = a + b + 1$ e $a \odot b = a + b + ab$. Mostre que $f: \mathbb{R} \to \mathbb{R}$ dado por $f(x) = x - 1$, $\forall x \in \mathbb{R}$ é um isomorfismo de $(\mathbb{R}, +, \cdot)$ em $(\mathbb{R}, \oplus, \odot)$. Defina o isomorfismo inverso.

**69.** Seja $A$ um anel com unidade. Para cada elemento inversível $a \in A$, seja $f_a: A \to A$ a aplicação dada pela lei $f_a(x) = axa^{-1}$. Mostre que $f_a$ é um isomorfismo e dê uma formula para $f_a \circ f_b$.

**70.** Seja $f: A \to B$ um isomorfismo de anéis. Mostre que:

a) Se $a \in A$ é um elemento idempotente, então $f(a)$ também o é.

b) Se $a \in A$ é nilpotente, então $f(a) \in B$ também o é.

c) Se $A$ possui unidade, $a \in A$ e $\exists\, b, c \in A$ $(b, c \notin U(A))$ tais que $a = b \cdot c$, então $f(a) \in$ $\in B$ pode também ser decomposto em dois fatores de $B$, ambos não inversíveis.

**71.** Mostre que nenhuma aplicação $f: A \to B$ em que $A = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$, $B = \{x + y\sqrt{3} \mid x, y \in \mathbb{Q}\}$ e $f\left(x + y\sqrt{2}\right) = x + y\sqrt{3}$ é um isomorfismo.
*Sugestão:* Observe que, se $f$ fosse um isomorfismo de $A$ em $B$, então $f\left(\sqrt{2}\right) =$ $a + b\sqrt{3}$. Calcule a seguir $f(2) = 2$ a partir de $f\left(\sqrt{2}\right) = a + b\sqrt{3}$.

**72.** Mostre que, se $f: \mathbb{Z} \to \mathbb{Z}$ é um isomorfismo de anéis, então $f$ é a aplicação idêntica de $\mathbb{Z}$.
*Sugestão:* Observe que $f(+1) = +1$ e que $\forall m \in \mathbb{Z}^*$ vale $m = (+1) + \ldots + (+1)$

**73.** Mostre que, se $f$ é um isomorfismo do anel $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ nele próprio, então $f\left(\sqrt{2}\right) = +\sqrt{2}$ ou $f\left(\sqrt{2}\right) = -\sqrt{2}$.

**74.** Mostre que, se $f: \mathbb{Q} \to \mathbb{Q}$ é um isomorfismo de anéis, então $f$ é a aplicação idêntica de $\mathbb{Q}$.
*Sugestão:* Observe que $f(1) = 1 = \left(\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}\right)$, $n$ vezes, $\forall n \in \mathbb{N}^*$. A partir disso calcule $f\left(\frac{1}{n}\right)$.

**75.** Determine todos os homomorfismos de $\mathbb{Z}$ em $\mathbb{Z}$.

**Resolução**

Seja $f: \mathbb{Z} \to \mathbb{Z}$ um homomorfismo tal que $f(1) = k$.

Provemos que $f(x) = kx$ para todo $x \in \mathbb{Z}$:

1º) $f(0) = 0 = k \cdot 0$.

2º) Se $f(n) = kn$, com $n \in \mathbb{N}$, então:

$f(n + 1) = f(n) + f(1) = kn + k = k(n + 1)$

Portanto, por indução, a tese está provada para todo $x \in \mathbb{N}$.

3º) Se $x \in \mathbb{Z}_-$, então $x = -|x|$ e $|x| \in \mathbb{Z}_+$, então:

$f(x) = f(-|x|) = -f(|x|) = -k|x| = k(-|x|) = kx$

Tendo provado que $f$ é uma função linear de $x$, determinemos agora o valor de $k$.

Como $f(x \cdot y) = f(x) \cdot f(y)$, para todo $x, y \in \mathbb{Z}$, temos:

$k(xy) = (kx) \cdot (ky)\ \forall x, y \in \mathbb{Z}$

E, daí

$k = k^2 \ \therefore \ k = 0$ ou $k = 1$

Conclusão: Há apenas dois homomorfismos do anel $\mathbb{Z}$ nele próprio: $f(x) = x$ e $f(x) = 0$. ■

**76.** Seja $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dada por por $f(x, y) = (mx + ny, px + qy)$.

a) Calcular $m, n, p, q$ de modo que $f$ seja um homomorfismo do anel $\mathbb{Z} \times \mathbb{Z}$ nele mesmo.

b) Em quais desses casos $f$ é um isomorfismo de $\mathbb{Z} \times \mathbb{Z}$?

**77.** Ache todos os homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_4$.

*Sugestão:* Considere as imagens possíveis de $1 \in \mathbb{Z}$ por um homomorfismo $f: \mathbb{Z} \to \mathbb{Z}_4$.

**78.** Ache todos os homomorfismos de $\mathbb{Z}$ em $\mathbb{Z}_6$.

**79.** Determine todos os homomorfismos do anel $\mathbb{Z}$ no anel $\mathbb{Z} \times \mathbb{Z}$.

**80.** Determine todos os homomorfismos de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$.

*Sugestão:* Faça $f(1, 0) = p$ e $f(0, 1) = q$; em seguida, note que $f(x, y) = f(x(1, 0) + y(0, 1))$.

### Exercícios complementares

**C4.** Mostre que $P = \{(a, b, -b, a) : a, b \in \mathbb{R}\}$, com a adição e a multiplicação definidas por

$$(a, b, -b, a) + (c, d, -d, c) = (a + c, b + d, -b - d, a + c)$$

$$(a, b, -b, a)(c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd)$$

é um corpo. Mostre que $P$ é isomorfo a $\mathbb{C}$, o corpo dos números complexos.

**C5.** Mostre que um homomorfismo de um corpo $K$ nele mesmo ou é a aplicação nula ou é um isomorfismo.

*Sugestão:* Faça $f(1) = a$ e analise as duas possibilidades, $a = 0$ ou $a \neq 0$.

# V-3 CORPO DE FRAÇÕES DE UM ANEL DE INTEGRIDADE

## 9. QUOCIENTES EM UM CORPO

Num corpo $K$, a equação $ax = b$, em que $a \neq 0$, tem uma única solução, que é o elemento $a^{-1}b = ba^{-1}$. Um elemento de $K$ escrito na forma $a^{-1}b = ba^{-1}$ é chama-

do *quociente* de $a$ por $b$ e denotado por $\frac{a}{b}$. É fácil ver, por outro lado, que todo elemento $a \in K$ é um quociente: por exemplo, se $b \neq 0$ é um elemento de $K$, então $a = (ab)b^{-1} = \frac{ab}{b}$.

Adotada a notação de quociente, as operações com elementos de um corpo se fazem segundo certas regras que facilitam os cálculos algébricos e que, num certo momento, nortearão nossos passos na construção do corpo de frações de um anel de integridade, nosso objetivo principal nesta seção. Vejamos como.

**Proposição 14:** Sejam $a, b, c, d$ elementos de um corpo $K$. Se $b \neq 0$ e $d \neq 0$, então:

(i) $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $ad = bc$;

(ii) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$;

(iii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

(iv) $-\frac{a}{b} = \frac{-a}{b}$;

(v) se $a \neq 0$ (além de $b$), então $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

*Demonstração:*

(i) Se $\frac{a}{b} = \frac{c}{d}$, então $ab^{-1} = cd^{-1}$. Daí, $ad = a(b^{-1}b)d = (ab^{-1})(bd) = (cd^{-1})(bd) = cb$.

Suponhamos, reciprocamente, que $ad = bc$. Então $\frac{a}{b} = ab^{-1} = a(dd^{-1})b^{-1} =$
$= (ad)(d^{-1}b^{-1}) = (bc)(d^{-1}b^{-1}) = cd^{-1} = \frac{c}{d}$.

(ii) $\frac{a}{b} \pm \frac{c}{d} = ab^{-1} \pm cd^{-1} = a(dd^{-1})b^{-1} \pm c(bb^{-1})d^{-1} = (ad)(bd)^{-1} \pm (bc)(bd)^{-1} =$
$= (ad \pm bc)(bd)^{-1} = \frac{ad \pm bc}{bd}$.

(iii) Fica como exercício.

(iv) $\frac{a}{b} + \frac{-a}{b} = \frac{ab + a(-b)}{bb} = \frac{0}{b^2} = 0 \cdot (b^2)^{-1} = 0$. Portanto, $\frac{-a}{b}$ é o oposto de $\frac{a}{b}$.

(v) Fica como exercício. #

## 10. CORPO DE FRAÇÕES DE UM ANEL DE INTEGRIDADE

A questão que temos pela frente agora é a seguinte: dado um anel de integridade $A$, construir um corpo $K$ do qual $A$ seja um subanel unitário. A construção que faremos é a mesma, no plano formal, pela qual se obtém o corpo dos números racionais a partir do anel dos inteiros.

Seja $A$ um anel de integridade. No conjunto $A \times A^*$ consideremos a relação $\sim$ definida da seguinte maneira:

$(a, b) \sim (c, d)$ se, e somente se, $ad = bc$.

Não é difícil provar que $\sim$ é uma relação de equivalência sobre $A \times A^*$. Por brevidade, mostraremos apenas que $\sim$ goza da propriedade transitiva.

De fato, consideremos $(a, b), (c, d), (e, f) \in A \times A^*$. Se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então $ad = bc$ e $cf = de$. Multiplicando os dois membros da primeira igualdade por $f$ e os dois da segunda por $b$, obtemos $adf = bcf$ e $bcf = bde$. Segue daí que $adf = bde$ e, portanto, cancelando-se $d$, o que é possível, pois $d \neq 0$ e $A$ é um anel de integridade, $af = be$. De onde, $(a, b) \sim (e, f)$.

Tratando-se de uma relação de equivalência muito especial, preferiremos usar a notação $\frac{a}{b}$ para representar a classe de equivalência determinada pelo par $(a, b)$, em vez da notação genérica $\overline{(a, b)}$. Os elementos do conjunto quociente $K = (A \times A^*)/\sim$, com a notação adotada, são as *frações* $\frac{a}{b}$ $(a \in A, b \in A^*)$. Então:

$\frac{a}{b} = \frac{c}{d}$ se, e somente se, $(a, b) \sim (c, d)$, se, e somente se, $ad = bc$.

Nosso objetivo é transformar $K$ num corpo. Inspirados nas considerações da seção anterior, definiremos "soma" e "produto" de duas frações, $\frac{a}{b}, \frac{c}{d} \in K$ da seguinte maneira:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{e} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Isso posto, pode-se provar que as definições dadas independem dos particulares pares escolhidos para representar as frações. Por exemplo, no caso da multiplicação, suponhamos $(a, b) \sim (m, n)$ e $(c, d) \sim (r, s)$. Então $an = bm$ e $cs = dr$. Multiplicando membro a membro essas igualdades, obtemos $(an)(cs) = (bm)(dr)$ e daí $(ac)(ns) = (bd)(mr)$. Isso significa, no presente contexto, que $(ac, bd) \sim (mr, ns)$ e, portanto, que $\frac{a}{b} \cdot \frac{c}{d} = \frac{m}{n} \cdot \frac{r}{s}$.

Rotineiramente se demonstra que $(K, +, \cdot)$ é um corpo. Destaquemos apenas alguns pontos dessa demonstração.

- *Associatividade* da adição:

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf}$$

Também:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}$$

Portanto

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}$$

- O zero do corpo é a fração $\frac{0}{1}$ (0 = zero de $A$; 1 = unidade de $A$), pois:

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}$$

- O oposto de uma fração $\frac{a}{b}$ é a fração $\frac{-a}{b}$.

- A unidade do corpo é a fração $\frac{1}{1}$.

- O inverso de uma fração $\frac{a}{b} \neq \frac{0}{1}$ é a fração $\frac{b}{a}$, pois:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}, \text{ uma vez que } (ab) \cdot 1 = 1 \cdot (ba)$$

O corpo $K$ assim obtido é chamado *corpo das frações* do anel de integridade $A$.

A seguir mostraremos de que maneira se pode considerar $A$ como um subanel unitário de $K$. Naturalmente, como os elementos e operações de $A$ e de $K$ têm natureza distinta, o sentido dessa afirmação é que há um subanel de $K$ que pode ser identificado com $A$ através de um isomorfismo conveniente. E, examinando o formato dos elementos de $K$, é lícito admitir que esse subanel possa ter como suporte o conjunto:

$$L = \left\{\frac{a}{1} \mid a \in K\right\}$$

Efetivamente, $L$ é um subanel de $K$, pois, tomando-se $\frac{a}{1}, \frac{b}{1} \in L$:

$$\frac{a}{1} - \frac{b}{1} = \frac{a}{1} + \left(-\frac{b}{1}\right) = \frac{a}{1} + \frac{-b}{1} = \frac{a + (-b)}{1} \in L$$

e

$$\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} \in L.$$

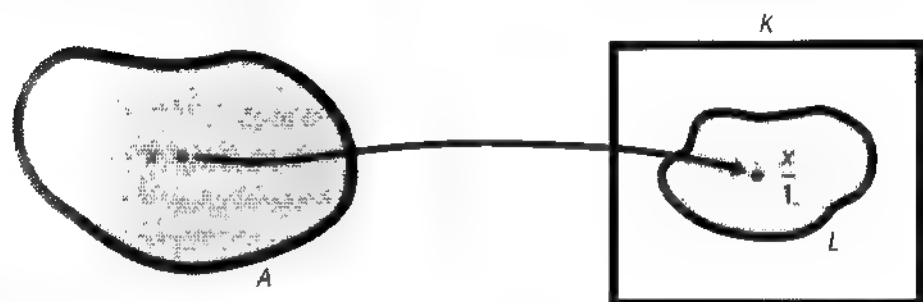
Para completar nossa argumentação, falta mostrar que a aplicação $f: A \to L$ que associa a cada elemento $a \in A$ a fração $\frac{a}{1}$ é um isomorfismo de anéis. De fato:

- $f(a + b) = \frac{a + b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$;

- $f(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a)f(b)$;

- se $f(a) = f(b)$, então $\frac{a}{1} = \frac{b}{1}$ e, portanto, $a \cdot 1 = 1 \cdot a$, ou seja, $a = b$, o que mostra que é injetora;

- se $y \in L$, então $y = \frac{a}{1}$, para um conveniente elemento $a \in A$ cuja imagem obviamente é $y$, pois $f(a) = \frac{a}{1} = y$, e isso prova que $f$ também é sobrejetora.

Assim, identificando $A$ com sua cópia $L = \left\{ \frac{a}{1} \mid a \in K \right\}$ em $K$, através do isomorfismo $f$, podemos dizer que $A$ é um subanel de $K$ e, inclusive, anotar $A \subset K$. Aliás, no plano formal, como já adiantamos de início, é com todos esses subentendidos que se considera $\mathbb{Z} \subset \mathbb{Q}$.

**Exercícios**

**81.** Sendo $A$ um corpo, define-se em $A \times A^*$ a relação de equivalência $(a, b) \mathrel{R} (c, d) \Leftrightarrow$
$\Leftrightarrow ad = bc$. Determine o corpo de frações de $A$.

**82.** Seja $A$ um subanel unitário de $\mathbb{Q}$. Determine o corpo de frações de $A$

**83.** Sejam $A$ e $B$ dois anéis de integridade isomorfos e seja $f: A \to B$ um isomorfismo. Mostre que existe um único isomorfismo $g: K \to L$, em que $K$ e $L$ são respectivamente os corpos de frações de $A$ e $B$, e $g$ um prolongamento de $f$.

**84.** Seja $p$ um número primo positivo. Seja $A = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}$. Mostre que $A$ é um subanel unitário de $\mathbb{Q}$ e determine o corpo de frações de $A$.

# V-4 CARACTERÍSTICA DE UM ANEL

## 11. INTRODUÇÃO

Consideremos o anel $\mathbb{Z}_m$ das classes de resto módulo $m$. Observemos que, qualquer que seja $\bar{a} \in \mathbb{Z}_m$:

$$m \cdot \bar{a} = \underbrace{\bar{a} + \bar{a} + \ldots + \bar{a}}_{(m \text{ parcelas})} = \overline{a + a + \ldots + a} = \overline{ma} = \bar{0}$$

uma vez que $ma \equiv 0 \pmod{m}$.

Essa propriedade do anel $\mathbb{Z}_m$ não é compartilhada pelos anéis numéricos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, por exemplo. De fato, considerando a unidade desses anéis, que é o número 1, então, qualquer que seja o inteiro estritamente positivo $m$:

$$m \cdot 1 = 1 + 1 + ... + 1 = m \neq 0$$

E essa diferença entre os anéis $\mathbb{Z}_m$ e os anéis numéricos não decorre apenas do fato de os primeiros serem finitos e estes infinitos. Mesmo num anel infinito $A$, pode ocorrer o seguinte:

$$m \cdot a = a + a + ... + a = 0 \text{ (zero do anel)}$$

para algum inteiro estritamente positivo $m$ e para todo elemento $a$ do anel, como teremos ocasião de mostrar (exemplo 39). Diga-se de passagem que, se $m \cdot a = 0$, então $(2m) \cdot a = (3m) \cdot a = ... = 0$.

Nosso objetivo nesta seção é explorar as possibilidades levantadas por essas observações para a teoria dos anéis. Mas para isso precisaremos explorar antes o conceito de *múltiplo de um elemento de um anel.*

## 12. MÚLTIPLOS DE UM ELEMENTO DE UM ANEL

Seja $(A, +, \cdot)$ um anel. Então $(A, +)$ é um grupo aditivo abeliano e, portanto, pode-se usar para seus elementos o conceito de *múltiplo* introduzido no capítulo IV (seção 9). Lembremos como, adaptando a notação ao presente caso: se $m$ é um inteiro e $a$ um elemento de $A$, então $m \cdot a$ é assim definido:

- se $m \geqslant 0$, por recorrência, da seguinte forma:

$$0 \cdot a = 0_A \text{ (zero de } A)$$
$$m \cdot a = (m - 1) \cdot a + a, \text{ se } m \geqslant 1$$

- se $m < 0$

$$m \cdot a = (-m) \cdot (-a)$$

O elemento $ma$ é chamado *múltiplo* m*-ésimo de a.*

Com base nessa definição, demonstram-se as seguintes propriedades (ver proposição 12, capítulo IV), válidas para qualquer $a \in A$ e quaisquer $m, n \in \mathbb{Z}$:

(i) $m \cdot a + n \cdot a = (m + n) \cdot a$;

(ii) $(-m) \cdot a = -(m \cdot a)$;

(iii) $n \cdot (m \cdot a) = (nm) \cdot a$.

Além dessas propriedades, há outra, de que precisaremos nesta seção, específica dos anéis com unidade.

**Proposição 15:** Seja $A$ um anel com unidade. Se $1_A$ indica a unidade e $m, n \in \mathbb{Z}$, então $(mn) \cdot 1_A = (m \cdot 1_A)(n \cdot 1_A)$.

*Demonstração.* Inicialmente suporemos $n \geqslant 0$. Para este caso, a demonstração será feita por indução sobre $n$.

Se $n = 0$, então $(mn) \cdot 1_A = 0 \cdot 1_A = 0_A$, ao passo que $(m \cdot 1_A)(n \cdot 1_A) = (m \cdot 1_A)(0 \cdot 1_A) = (m \cdot 1_A)0_A = 0_A$. Portanto, a igualdade vale quando $n = 0$.

Seja $r$ um inteiro maior que ou igual a 0 e suponhamos $(mr) \cdot 1_A = (m \cdot 1_A)(r \cdot 1_A)$.

Então $[m(r + 1)] \cdot 1_A = (mr + m) \cdot 1_A = (mr) \cdot 1_A + m \cdot 1_A = (m \cdot 1_A)(r \cdot 1_A) + m \cdot 1_A = (m \cdot 1_A)(r \cdot 1_A) + (m \cdot 1_A)1_A = (m \cdot 1_A)(r \cdot 1_A + 1_A) = (m \cdot 1_A)[(r + 1) \cdot 1_A]$.

Com isso a propriedade está demonstrada para $n \geqslant 0$.

Suponhamos $n < 0$. Então:

$(mn) \cdot 1_A = [(-m)(-n)] \cdot 1_A = [(-m) \cdot 1_A][(-n) \cdot 1_A] = [-(m \cdot 1_A)][-(n \cdot 1_A)] = (m \cdot 1_A)(n \cdot 1_A)$ #

**Corolário:** Seja $A$ um anel com unidade. Então o conjunto $B = \mathbb{Z} \cdot 1_A = \{m \cdot 1_A \mid m \in \mathbb{Z}\}$ é um subanel unitário de $A$.

*Demonstração:* Como $1_A = 1 \cdot 1_A$, então $1_A \in B$ que, portanto, não é vazio. Sejam $m \cdot 1_A, n \cdot 1_A \in B$. Então:

- $m \cdot 1_A - n \cdot 1_A = m \cdot 1_A + [-(n \cdot 1_A)] = m \cdot 1_A + [(-n) \cdot 1_A] = [m + (-n)] \cdot 1_A = (m - n) \cdot 1_A$, o que mostra que $B$ é fechado para a subtração;
- $(m \cdot 1_A)(n \cdot 1_A) = (mn) \cdot 1_A$, o que mostra que $B$ é fechado para a multiplicação.

Então $B = \mathbb{Z} \cdot 1_A$ é um subanel de $A$, unitário, porque $1_A \in B$, como já observamos. #

## 13. CARACTERÍSTICA DE UM ANEL

**Definição 15:** Seja $A$ um anel. Suponhamos que, para algum inteiro $n > 0$ e para qualquer $a \in A$, verifica-se a igualdade $n \cdot a = 0$ (zero do anel). Então existe um menor inteiro estritamente positivo $r$ tal que $r \cdot a = 0$, qualquer que seja $a \in A$. Esse inteiro $r$ é chamado *característica* do anel $A$ e indicado por $c(A)$. Se, ao contrário, o anel $A$ possui pelo menos um elemento $a$ tal que $n \cdot a \neq 0$, qualquer que seja o inteiro estritamente positivo $n$, então se diz que a *característica* do anel é 0.

*Exemplo 37:* Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica 0, pois, se $m \neq 0$, então $m \cdot 1 = m$ e, portanto, $m \cdot 1 \neq 0$.

**Proposição 16:** Seja $A$ um anel com unidade. Então a característica de $A$ é um inteiro $h > 0$ se, e somente se, $h$ é o menor inteiro estritamente positivo tal que $h \cdot 1_A = 0_A$. Ou seja, se, e somente se, $h$ é a ordem de $1_A$ no grupo aditivo $(A, +)$.

*Demonstração:*

$(\rightarrow)$ Por hipótese, $c(A) = h$. Portanto, $h \cdot a = 0_A$, qualquer que seja $a \in A$. Em particular, $h \cdot 1_A = 0_A$. Suponhamos que, para algum inteiro $m$, $0 < m < h$, se pudesse ter $m \cdot 1_A = 0_A$. Então, qualquer que seja $a \in A$:

$$m \cdot a = a + a + ... + a = a1_A + a1_A + ... + a1_A$$
$$= a(1_A + 1_A + ... + 1_A) = a(m \cdot 1_A) = a0_A = 0_A$$

o que é absurdo, uma vez que $c(A) = h$.

(⇐) Por hipótese, $h$ é o menor inteiro estritamente positivo tal que $h \cdot 1_A = 0_A$. Então, qualquer que seja $a \in A$:

$h \cdot a = a + a + ... + a = a1_A + a1_A + ... + a1_A = a(1_A + 1_A + ... + 1_A) = a(h \cdot 1_A) = a0_A = 0_A$

Se houvesse algum inteiro $m$ tal que $0 < m < h$ e $m \cdot a = 0_A$, para qualquer $a \in A$, então, em particular, $m \cdot 1_A = 0$, o que é contrário à hipótese. #

*Exemplo 38:* Observemos primeiro que, em $\mathbb{Z}_m$, $m \cdot \bar{1} = \bar{1} + \bar{1} + ... + \bar{1} = \bar{m} = \bar{0}$. Suponhamos, por outro lado, que para algum inteiro $r$, $0 < r < m$, se tivesse $r \cdot \bar{1} = \bar{0}$. Como $r \cdot \bar{1} = \bar{r}$, então $\bar{r} = \bar{0}$, ou seja, $r \equiv 0 \pmod m$. Então $m \mid r$, o que é impossível, uma vez que $0 < r < m$. Logo, $c(\mathbb{Z}_m) = m$.

**Proposição 17:** Se a característica de um anel de integridade $A$ não é zero, então é um número primo.

*Demonstração:* Seja $c(A) = h > 0$. Se $h$ não fosse um número primo, então $h = rs$, para um par conveniente de inteiros $r$ e $s$ tais que $1 < r, s < h$. Como $c(A) = h$, então $r \cdot 1_A \neq 0_A$ e $s \cdot 1_A \neq 0_A$. Mas $0_A = h \cdot 1_A = (rs) \cdot 1_A = (r \cdot 1_A)(s \cdot 1_A)$.

Da igualdade $(r \cdot 1_A)(s \cdot 1_A) = 0_A$ obtida, segue que os elementos $r \cdot 1_A$ e $s \cdot 1_A$ são divisores próprios do zero em $A$, o que contraria a hipótese de que $A$ é um anel de integridade. Portanto, $h$ é primo. #

*Exemplo 39:* Vamos dar agora um exemplo de um anel comutativo com unidade e infinito cuja característica é 2. Esse anel é formado por todas as seqüências infinitas de elementos de $\mathbb{Z}_2$ com a adição e a multiplicação definidas componente a componente. Se indicarmos por $A$ esse anel, então:

$$A = \{(a_1, a_2, ..., ...) \mid a_1, a_2, ... \in \mathbb{Z}_2\}$$
$$(a_1, a_2, ...) + (b_1, b_2, ...) = (a_1 + b_1, a_2 + b_2, ...)$$
$$(a_1, a_2, ...)(b_1, b_2, ...) = (a_1b_1, a_2b_2, ...)$$

Deixamos para o leitor a verificação de que realmente se trata de um anel comutativo com unidade. Apenas destacamos que o zero desse anel é a seqüência $(\bar{0}, \bar{0}, ..., \bar{0}, ...)$ e a unidade a seqüência $(\bar{1}, \bar{1}, ..., \bar{1}, ...)$. Como

$$2 \cdot (\bar{1}, \bar{1}, ..., \bar{1}, ...) = (\bar{1}, \bar{1}, ..., \bar{1}, ...) + (\bar{1}, \bar{1}, ..., \bar{1}, ...) = (\bar{2}, \bar{2}, ..., \bar{2}, ...) = (\bar{0}, \bar{0}, ..., \bar{0}, ...)$$

e, obviamente,

$$1 \cdot (\bar{1}, \bar{1}, ..., \bar{1}, ...) = (\bar{1}, \bar{1}, ..., \bar{1}, ...) \neq (\bar{0}, \bar{0}, ..., \bar{0}, ...)$$

então $c(A) = 2$.

*Exemplo 40:* A característica de um anel com unidade finito é maior que zero. Indiquemos por $A$ esse anel e consideremos a sequência

$$1_A, 2 \cdot 1_A, 3 \cdot 1_A, ...$$

O fato de $A$ ser finito assegura que há dois elementos nessa sequência, digamos, $r \cdot 1_A$ e $s \cdot 1_A$ tais que $r > s$ e $r \cdot 1_A = s \cdot 1_A$ e, portanto, $(r - s) \cdot 1_A = 0_A$, com $r - s > 0$. O menor inteiro estritamente positivo $h$ tal que $h \cdot 1_A = 0_A$ é a característica de $A$.

**Proposição 18:** Dois anéis isomorfos têm a mesma característica.

*Demonstração:* Sejam $A$ e $B$ os anéis e indiquemos por $f: A \rightarrow B$ o isomorfismo. Suponhamos primeiro que $c(A) = h$ e tomemos $b \in B$. Como $f$ é sobrejetora, então $b = f(a)$, para algum $a \in A$. Então:

$$h \cdot b = h \cdot f(a) = f(a) + f(a) + ... + f(a) = f(a + a + ... + a) = f(h \cdot a) = f(0_A) = 0_B$$

Suponhamos que para algum inteiro $s$, $0 < s < h$, pudesse ocorrer a igualdade $s \cdot b = 0_B$, qualquer que fosse o elemento $b \in B$. Isso posto, seja $a$ um elemento arbitrário de $A$. Como $a = f^{-1}(f(a))$, em que $f^{-1}$ é o isomorfismo inverso de $f$, então:

$$s \cdot a = s \cdot [f^{-1}(f(a))] = f^{-1}(f(a)) + f^{-1}(f(a)) + ... + f^{-1}(f(a)) =$$
$$= f^{-1}[f(a) + f(a) + ... + f(a)] = f^{-1}(s \cdot f(a)) = f^{-1}(0_B) = 0_A$$

o que é impossível, pois $c(A) = h$. Das duas conclusões, segue que $c(B) = h$. #

Deixamos como exercício a demonstração no caso em que $c(A) = 0$.

O corolário da proposição 15 nos diz que, se $A$ é um anel com unidade, então $\mathbb{Z} \cdot 1_A = \{m \cdot 1_A \mid m \in \mathbb{Z}\}$ é um subanel unitário de $A$. Se a característica de $A$ é $h > 0$, então $h \cdot 1_A = 0_A$ e os elementos $0 \cdot 1_A = 0_A, 1 \cdot 1_A, ..., (h - 1) \cdot 1_A$ são distintos entre si. De fato, a suposição $r \cdot 1_A = s \cdot 1_A$, com $0 \leqslant s < r < h$, levaria à igualdade $(r - s) \cdot 1_A = 0_A$, em que $0 < r - s < h$, o que é impossível, considerando-se que $c(A) = h$. Mais: não há nenhum outro elemento em $\mathbb{Z} \cdot 1_A$, além daqueles relacionados. Para provar essa afirmação, que equivale a dizer que $\mathbb{Z} \cdot 1_A = \{0 \cdot 1_A = 0_A, 1 \cdot 1_A, ..., (h - 1) \cdot 1_A\}$, seja $m \cdot 1_A \in \mathbb{Z} \cdot 1_A$. Aplicando-se o algoritmo euclidiano de $\mathbb{Z}$ com $m$ como dividendo e $h$ como divisor:

$$m = hq + r \ (0 \leqslant r < h)$$

Então:

$$m \cdot 1_A = (hq + r) \cdot 1_A = (hq) \cdot 1_A + r \cdot 1_A = (h \cdot 1_A)(q \cdot 1_A) + r \cdot 1_A =$$
$$= 0_A(q \cdot 1_A) + r \cdot 1_A = 0_A + r \cdot 1_A = r \cdot 1_A \ (0 \leqslant r < h)$$

Ou seja, $m \cdot 1_A$ é um dos elementos da sucessão $0 \cdot 1_A = 0_A, 1 \cdot 1_A, ..., (h - 1) \cdot 1_A$, como queríamos demonstrar. Portanto, neste caso, $\mathbb{Z} \cdot 1_A$ tem o mesmo cardinal de $\mathbb{Z}_h$.

E se $c(A) = 0$, então não há elementos repetidos em $\mathbb{Z} \cdot 1_A$. De fato, a suposição $r \cdot 1_A = s \cdot 1_A$, com $s < r$, levaria à igualdade $(r - s) \cdot 1_A = 0_A$, em que $r - s > 0$. Fazendo-se $r - s = t$, então, qualquer que seja $a \in A$:

$$t \cdot a = a + a + ... + a = a1_A + a1_A + ... + a1_A = a(1_A + 1_A + ... + 1_A) = a(t \cdot 1_A) = a0_A = 0_A$$

o que é impossível, pois $c(A) = 0$. Portanto, neste caso,

$$\mathbb{Z} \cdot 1_A = \{0_A, (\pm 1) \cdot 1_A, (\pm 2) \cdot 1_A, ..., (\pm n) \cdot 1_A, ...\}$$

tem o mesmo cardinal de $\mathbb{Z}$.

Essas considerações e propriedades já vistas para os múltiplos de um elemento de um anel, particularmente os múltiplos da unidade, indicam a possibilidade de um isomorfismo entre $\mathbb{Z}_h$ e $\mathbb{Z} \cdot 1_A$ (via $r \to r \cdot 1_A$), no caso em que $c(A) = h > 0$, e entre $\mathbb{Z}$ e $\mathbb{Z} \cdot 1_A$ (via $r \to r \cdot 1_A$), no caso em que $c(A) = 0$. E, de fato, é isso o que acontece, como se mostrará a seguir.

**Proposição 19:** Seja $A$ um anel com unidade. (i) Se $c(A) = h > 0$, então a correspondência que associa a cada $\overline{r} \in \mathbb{Z}_h$ o elemento $r \cdot 1_A \in \mathbb{Z} \cdot 1_A$ é um isomorfismo de anéis. (ii) E se $c(A) = 0$, então é um isomorfismo de anéis a aplicação $f: \mathbb{Z} \to \mathbb{Z} \cdot 1_A$ definida por $f(r) = r \cdot 1_A$.

*Demonstração:*

(i) Observemos que $\overline{r} = \overline{s}$ se, e somente se, $h \mid (r - s)$;
se, e somente se, $r - s = ht$ $(t \in \mathbb{Z})$.

Logo, $(r - s) \cdot 1_A = (ht) \cdot 1_A = (h \cdot 1_A)(t \cdot 1_A) = 0_A(t \cdot 1_A) = 0_A$. Como $(r - s) \cdot 1_A = r \cdot 1_A - s \cdot 1_A$, então $r \cdot 1_A = s \cdot 1_A$. Portanto, a correspondência $r \to r \cdot 1_A$ é uma aplicação de $\mathbb{Z}_h$ em $\mathbb{Z} \cdot 1_A$. Dando a ela o nome de $g$, mostremos que se trata de um isomorfismo.

Nas considerações que antecedem essa proposição está desenvolvido o raciocínio que mostra que $g$ é uma bijeção. Por último:

- $g(\overline{r} + \overline{s}) = g(\overline{r + s}) = (r + s) \cdot 1_A = r \cdot 1_A + s \cdot 1_A = g(\overline{r}) + g(\overline{s})$;
- $g(\overline{rs}) = (rs) \cdot 1_A = (r \cdot 1_A)(s \cdot 1_A) = g(\overline{r})g(\overline{s})$.

(ii) Fica como exercício. O raciocínio é essencialmente o mesmo. #

Essa proposição nos autoriza a considerar $\mathbb{Z}_h$ como subanel de todo anel $A$ com unidade de característica $h > 0$, o que naturalmente pressupõe a identificação de $\mathbb{Z}_h$ com $\mathbb{Z} \cdot 1_A$, justificada pelo isomorfismo $g$. E também a considerar $\mathbb{Z}$ como subanel de todo anel com unidade de característica zero, através da identificação de $\mathbb{Z}$ com $\mathbb{Z} \cdot 1_A$, justificada neste caso pelo isomorfismo $f$.

## 14. CARACTERÍSTICA DE UM CORPO

Se $K$ é um corpo, então $c(K) = p$ (primo) ou $c(K) = 0$, uma vez que todo corpo é um anel de integridade. No primeiro caso, como acabamos de ver, o corpo $K$ contém $\mathbb{Z}_p$, que, pelo fato de $p$ ser primo, também é um corpo. Ou seja, $\mathbb{Z}_p$ é um subcorpo de $K$. Mas, como a unidade $1_K$ (ou 1, pela identificação feita) pertence a todo subcorpo $L$ de $K$, então $m \cdot 1_K \in L$, qualquer que seja o inteiro $m$, e, portanto, $\mathbb{Z}_p$ está contido em todo subcorpo de $K$. Ou seja, $\mathbb{Z}_p$ é o "menor" subcorpo de $K$.

No caso de $c(K) = 0$, pode-se demonstrar que o "menor" subcorpo de $K$ é $\mathbb{Q}$. Para justificar essa afirmação, seja $f: \mathbb{Q} \to K$ assim definida: $f\left(\frac{m}{n}\right) = \frac{m \cdot 1_k}{n \cdot 1_k}$. Então:

- $\dfrac{m \cdot 1_k}{n \cdot 1_k} = \dfrac{r \cdot 1_k}{s \cdot 1_k}$ se, e somente se, $(m \cdot 1_k)(s \cdot 1_k) = (n \cdot 1_k)(r \cdot 1_k)$;
se, e somente se, $(ms) \cdot 1_k = (nr) \cdot 1_k$,
se, e somente se, $(ms - nr) \cdot 1_K = 0_K$;
se, e somente se, $ms - nr = 0$ (pois $c(K) = 0$);
se, e somente se, $ms = nr$;
se, e somente se, $\dfrac{m}{n} = \dfrac{r}{s}$.

Isso prova que $f$ é injetora. Ademais:

- $f\left(\dfrac{m}{n} + \dfrac{r}{s}\right) = f\left(\dfrac{ms + nr}{ns}\right) = \dfrac{(ms + nr) \cdot 1_k}{(ns) \cdot 1_k} = \dfrac{(m \cdot 1_k)(s \cdot 1_k) + (n \cdot 1_k)(r \cdot 1_k)}{(n \cdot 1_k)(s \cdot 1_k)} =$

$= \dfrac{m \cdot 1_k}{n \cdot 1_k} + \dfrac{r \cdot 1_k}{s \cdot 1_k} = f\left(\dfrac{m}{n}\right) + f\left(\dfrac{r}{s}\right).$

- De maneira análoga se demonstra que $f$ preserva a multiplicação.

Sendo $f$ um homomorfismo injetor, então $Im(f) = \left\{\dfrac{m \cdot 1_k}{n \cdot 1_k} \mid \dfrac{m}{n} \in \mathbb{Q}\right\}$ é um subcorpo de $K$, como já vimos (seção 8). Portanto, podemos considerar $\mathbb{Q}$, (identificado com $Im(f)$) como um subcorpo de $K$ E é o menor subcorpo de $K$ pela razão seguinte: se $L$ é um subcorpo de $K$, então $1_k \in L$; daí, $m \cdot 1_k, n \cdot 1_k \in L$, quaisquer que sejam $m, n \in \mathbb{Z}$, com $n \neq 0$, portanto, $(m \cdot 1_k)(n \cdot 1_k)^{-1} = \dfrac{m \cdot 1_k}{n \cdot 1_k} \in L$.

Os corpos $\mathbb{Z}_p$ e $\mathbb{Q}$, pilares fundamentais sobre os quais assentam todos os corpos, os de característica maior que 0 no primeiro caso e os de característica zero no segundo, são chamados *corpos primos*.

## Exercícios

**85.** Determine as características dos seguintes anéis:

a) $\mathbb{Z}_3$
b) $\mathbb{Z}$
c) $\mathbb{Z} \times \mathbb{Z}$
d) $\mathbb{Z}_2 \times \mathbb{Z}$
e) $\mathbb{Z}_6 \times \mathbb{Z}_8$
f) $\mathbb{R}^{\mathbb{R}}$

**86.** Determine a característica do anel das matrizes reais do tipo $n \times n$ sobre $\mathbb{R}$ e sobre $\mathbb{Z}_5$.

**87.** Sejam $A$ e $B$ dois anéis comutativos com elementos unidades. Demonstre que a característica do anel produto direto $A \times B$ é igual ao mmc das característica de $A$ e de $B$.

**88.** Ache um anel de característica zero e um elemento $a$ não nulo desse anel de forma que $n \cdot a = 0$ para um certo $n \in \mathbb{N}^*$.
*Sugestão:* Tome, por exemplo, $A = \mathbb{Z}_2 \times \mathbb{Z}$

**89.** Pode um anel finito ter característica zero? Prove ou contra-exemplifique.

**90.** Dê um exemplo de um anel infinito cuja característica seja diferente de zero.

**91.** Pode um anel com unidade ter característica 1? Por quê?

**92.** Mostre que um anel de integridade com quatro elementos tem característica 2.
*Sugestão:* Raciocine em termos do período da unidade, no que se refere à adição

**93.** Seja $A$ um anel cuja característica é um número natural $n > 0$ não primo.
Mostre que $A$ possui divisores próprios do zero.

**94.** Seja $A$ um anel com unidade tal que $x^2 = x, \forall x \in A$.
Mostre que $c(A) = 2$ e $A$ é comutativo.

**95.** Seja $A$ um anel e $L$ um subanel de $A$. Mostre que $c(L) \leqslant c(A)$.
Dê um exemplo de um anel $A$ e um subanel $L$ de $A$ para os quais $c(L) < c(A)$.

**96.** Seja $f: A \to B$ um homomorfismo sobrejetor de anéis. Mostre que $c(B) \geqslant c(A)$.

**97.** Seja $K$ um corpo finito de característica $p > 0$. Mostre que a aplicação $f: K \to K$ definida por $f(x) = x^p$ é um isomorfismo de $K$.

**98.** a) Mostre que os subconjuntos $S = \{\bar{0}, \bar{5}, \overline{10}\}$ e $T = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}\}$ do anel $\mathbb{Z}_{15}$ são anéis de integridade relativamente às operações em $\mathbb{Z}_{15}$, induzidas sobre eles.
b) Mostre que $S$ é isomorfo a $\mathbb{Z}_3$. Qual é a característica de $S$?
c) Mostre que $T$ é um corpo de característica 5.

## Exercícios complementares

**C6.** Mostre que o número de elementos de um corpo de característica $p$ é uma potência de $p$.

**C7.** Mostre que, se $K$ é um corpo de característica $p > 0$, então $(x + y)^p = x^p + y^p$ para todos $x, y \in K$

# V-5 IDEAIS EM UM ANEL COMUTATIVO

## 15. NOTA HISTÓRICA

O "último teorema de Fermat" , desde sua formulação, feita na primeira metade do século XVII, até sua demonstração, realizada finalmente em 1994 pelo inglês Andrew Wiles, sempre foi um desafio intrigante, até para leigos. No século XIX, muitos matemáticos deram contribuições para a resolução desse problema, porém talvez nenhum mais do que o alemão Ernst Kummer (1810-1893).

Em 1843, Kummer chegou a submeter uma pretensa demonstração do teorema ao seu conterrâneo P. G. L. Dirichlet (1805-1859). Mas este enxergou um erro na demonstração: sem fundamento, o matemático utilizara uma generalização do teorema fundamental da aritmética para um certo tipo de "inteiros" envolvidos na demonstração. Kummer retornou ao problema com mais empenho ainda e acabou encontrando uma resposta para a questão da "fatoração única" levantada por suas pesquisas. Para isso, introduziu um "outro tipo de números", a que chamou *números ideais* e que não chegou a definir genericamente, e com esses novos números conseguiu restabelecer a fatoração única. Acrescente-se que Kummer deu uma demonstração parcial, mas muito ampla, do teorema de Fermat, para uma categoria infinita de expoentes primos.

Em 1871, R. Dedekind mostrou que os fatores ideais de Kummer poderiam ser substituídos por classes de números algébricos, as quais, em consideração a Kummer, chamou de *ideais*. Dedekind, definiu *ideal* em um corpo de números algébricos $K$ como um subconjunto $A \subset K$ que goza da seguinte propriedade:

Se $a, b \in A$ e $m, n \in \mathbb{Z}$, então $ma + nb \in A$.

Com isso, ele transferiu o problema da fatoração única para o conjunto dos ideais e, com o conceito de *ideal primo* (definição 18, desta seção), também conseguiu, por um caminho matematicamente muito mais produtivo, restabelecer a fatoração única.

O conceito de ideal, generalizado para anéis quaisquer, é um dos instrumentos mais poderosos para o desenvolvimento da teoria dos anéis, como poderá ser observado na seqüência deste trabalho. E suas aplicações em áreas diversas, como, por exemplo, no estudo das curvas algébricas, fazem dele um dos mais importantes da matemática moderna.

## 16. IDEAIS EM UM ANEL COMUTATIVO

O conceito de ideal pode ser introduzido em relação a um anel qualquer, porem

---

Essencialmente, o teorema afirma que não há nenhum terno de números inteiros estritamente positivos que seja solução de $x^n + y^n = z^n$ quando $n > 2$. Vale lembrar que quando $n = 1$ ou $n = 2$ essa equação tem infinitas soluções, constituídas de componentes estritamente positivos.

nos ateremos aos anéis comutativos, dada sua importância maior neste caso e as limitações que os objetivos deste trabalho impõem.

**Definição 16:** Seja $A$ um anel comutativo. Um subconjunto $I \subset A, I \neq \varnothing$, será chamado de *ideal* em $A$ se, para quaisquer $x, y \in I$ e para qualquer $a \in A$, verificarem-se as relações seguintes. (i) $x - y \in I$; (ii) $ax \in I$

*Exemplo 41:* Se $A$ indica um anel comutativo, então $\{0_A\}$ e o próprio $A$ são ideais em $A$. São os *ideais triviais* do anel

*Exemplo 42.* No anel $\mathbb{Z}$, os subconjuntos $n\mathbb{Z} = \{0, \pm n, \pm 2n, ...\}$, qualquer que seja o inteiro $n$. De fato:

- se $x, y \in n\mathbb{Z}$, então $x = rn$ e $y = sn$, para convenientes inteiros $r$ e $s$. Logo, $x - y =$ $= rn - sn = (r - s)n$, em que $r - s$ é inteiro. De onde, $x - y \in n\mathbb{Z}$;
- sejam $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$; então $x = nq$ $(q \in \mathbb{Z})$ e, portanto, $ax = a(nq) = (aq)n$, em que $aq$ é inteiro, o que mostra que $ax \in n\mathbb{Z}$.

Pode-se provar reciprocamente que, se $I$ é um ideal em $\mathbb{Z}$, então $I$ possui um elemento $n$ tal que $I = n\mathbb{Z}$. Esse resultado é o objeto do exemplo 45.

*Exemplo 43:* O núcleo de um homomorfismo de anéis $f: A \to B$ é um ideal em $A$. Lembremos que $N(f) = \{a \in A \mid f(a) = 0_B\}$.

- Como $f(0_A) = 0_B$, então $0_A \in A$ e, portanto, $N(f) \neq \varnothing$.
- Se $x, y \in N(f)$, então $f(x) = f(y) = 0_B$; logo, $f(x - y) = f(x) - f(y) = 0_B - 0_B =$ $= 0_B$ e, portanto, $x - y \in N(f)$.
- Se $x \in N(f)$, então $f(x) = 0_B$ e, portanto, qualquer que seja $a \in A$, $f(ax) =$ $= f(a)f(x) = f(a)0_B = 0_B$, o que mostra que $ax \in N(f)$.

*Exemplo 44:* No anel $A = \mathbb{R}^{\mathbb{R}}$ é um ideal o subconjunto $I = \{f: \mathbb{R} \to \mathbb{R} \mid f(1) = 0\}$. Considerando-se que obviamente $I$ é diferente do vazio, sejam $f, g \in I$. Então:

$$(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$$

e, portanto, $f - g \in I$. Agora, se $h \in A$ e $f \in I$, então:

$$(hf)(1) = h(1)g(1) = h(1) \cdot 0 = 0$$

o que garante que $hf \in I$ e, portanto, completa a demonstração de que $I$ é um ideal em $A = \mathbb{R}^{\mathbb{R}}$.

Um ideal $I$ num anel $A$ certamente é um subanel de $A$. De fato, se $x, y \in I$, então $x - y \in I$, devido à definição de ideal, e $xy \in I$, também devido à definição, uma vez que, se $x \in I$, então, $x \in A$ Mas não vale a recíproca dessa propriedade. De fato, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, como já vimos, mas não é um ideal em $\mathbb{Q}$, uma vez que, por exemplo, $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$ mas $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

**Proposição 20:** Seja $J$ um ideal em um anel comutativo $A$. Então:

(i) $0 \in J$ ($0$ − zero do anel).

(ii) Se $a \in J$, então $\quad a \in J$.

(iii) Se $a, b \in J$, então $a + b \in J$.

(iv) Se o anel possui unidade e se algum elemento inversível do anel pertence a $J$, então $J = A$.

*Demonstração:*

(i) Seja $a \in J$ (lembrar que $J \neq \varnothing$, por definição). Logo, $a \quad a \in J$, ou seja, $0 \in J$.

(ii) Como $0 \in J$ (devido a (i)) e $a$ é um elemento do ideal, então $0 \quad a \quad a \in J$.

(iii) Por hipótese, $a, b \in J$. Mas, se $b \in J$, então $-b \in J$, como acabamos de ver. Logo, devido à definição, $a - (-b) = a + b \in J$.

(iv) Como $J \subset A$, basta mostrar que $A \subset J$. Para isso tomemos um elemento genérico $a$ do anel. Obviamente $a = a \cdot 1$ ($1$ = unidade do anel). Tomando-se um elemento inversível $u \in J$, o que é garantido pela hipótese, então, para algum $v \in A$, $uv = 1$ (unidade do anel). Portanto:

$$a = a \cdot 1 = a(uv) = (av)u$$

Observando-se que $av \in A$ e $u \in J$, então $a = (av)u \in J$. Se todo elemento de $A$ pertence a $J$ então $A \subset J$, como queríamos demonstrar. #

## 17. IDEAIS GERADOS POR UM NÚMERO FINITO DE ELEMENTOS

Para quaisquer $n$ elementos $a_1, a_2, ..., a_n$ ($n \geqslant 1$) de um anel comutativo $A$, indicaremos por $\langle a_1, a_2, ..., a_n \rangle$ o seguinte subconjunto de $A$:

$$\langle a_1, a_2, ..., a_n \rangle = \{x_1a_1 + x_2a_2 + ... + x_na_n \mid x_1, x_2, ..., x_n \in A\}$$

Provemos que $\langle a_1, a_2, ..., a_n \rangle$ é um ideal em $A$. De fato:

- $0 = 0a_1 + 0a_2 + ... + 0a_n \in \langle a_1, a_2, ..., a_n \rangle$ e, portanto, esse conjunto não é vazio.
- Se $b, c \in \langle a_1, a_2, ..., a_n \rangle$, então $b = x_1a_1 + ... + x_na_n$ e $c = y_1a_1 + ... + y_na_n$, em que os $x_i$ e os $y_i$ ($1 \leqslant i \leqslant n$) são convenientes elementos de $A$; observando que $(x_i - y_i) \in A$, ($i = 1, 2, ..., n$) e que $b - c = (x_1 - y_1)a_1 + ... + (x_n - y_n)a_n$, concluímos que $b - c \in \langle a_1, a_2, ..., a_n \rangle$.
- Se $b$ é um elemento de $\langle a_1, a_2, ..., a_n \rangle$, digamos, $b = x_1a_1 + ... + x_na_n$, e se $c \in A$, então:

$$cb = (cx_1)a_1 + ... + (cx_n)a_n \in \langle a_1, a_2, ..., a_n \rangle$$

pois cada um dos produtos $cx_i$ pertence a $A$.

**Definição 17:** Se $A$ é um anel comutativo e $S = \{a_1, a_2, ..., a_n\} \subset A$, então o ideal $\langle a_1, a_2, ..., a_n \rangle$, introduzido nas considerações anteriores, é chamado *ideal gerado por* $S$ (ou pelos elementos de $S$). O ideal gerado por um conjunto unitário $\{a\}$ é chamado *ideal principal gerado por* a. Se todos os ideais de um anel comutativo são principais, então esse anel recebe o nome de *anel principal*

*Exemplo 45:* O anel $\mathbb{Z}$ é principal. Seja $I$ um ideal em $\mathbb{Z}$. Se $I = \{0\}$, então é imediato que $I$ é principal, pois $\langle 0 \rangle = \{x \cdot 0 \mid x \in \mathbb{Z}\} \quad \{0\}$ Se $I \neq \{0\}$, então $I$ possui um elemento não nulo $a$ e, portanto, $\quad a \in A$ Como um desses dois elementos ($a$ ou $\quad a$) é estritamente positivo, então $A$ possui elementos estritamente positivos, o menor dos quais indicaremos por $b$. Nosso propósito agora é provar que $I = \langle b \rangle$, o que concluirá a justificação.

Como $b \in I$, então $\langle b \rangle \subset I$. Para demonstrar a inclusão contrária, tomemos um elemento genérico $m \in I$ e apliquemos o algoritmo euclidiano ao par formado por esse elemento, como dividendo, e $b$, como divisor. Se $q$ é o quociente e $r$ o resto:

$$m = bq + r \ (0 \leqslant r < b)$$

Segue dessa igualdade que:

$$r = m - bq$$

e, portanto, que $r \in I$, uma vez que $m, b \in I$ e $I$ é um ideal. Mas, como $b$ é o menor inteiro estritamente positivo que pertence a $I$ e $r < b$, não se pode ter $r > 0$. Logo, $r = 0$ e, portanto, $m = bq$, o que mostra que $m \in \langle b \rangle$. Portanto, $I \subset \langle b \rangle$.

As duas inclusões demonstradas garantem que $I \quad \langle b \rangle$.

*Exemplo 46:* Vamos mostrar que o conjunto $I = \{x \in \mathbb{Z} \mid 9 \text{ divide } 21x\}$ é um ideal em $\mathbb{Z}$ e encontrar seu gerador.

O número 0, por exemplo, pertence a $I$, pois $9 \mid 0$

Se $x, y \in I$, então $9 \mid 21x$ e $9 \mid 21y$ e, portanto, 9 é divisor de $21x \quad 21y = 21(x \quad y)$, igualdade que mostra que $(x \quad y) \in I$.

Se $x \in I$, então $9 \mid 21x$ e daí segue que $9 \mid 21(ax)$, qualquer que seja $a \in \mathbb{Z}$, ou seja, $ax \in I$.

Sendo um ideal em $\mathbb{Z}$, então $I$ é gerado pelo menor de seus elementos estritamente positivos. Uma verificação direta mostra que esse elemento é o número 3. Portanto, $I = \langle 3 \rangle$.

**Proposição 21:** Seja $A$ um anel comutativo com unidade. Então $A$ é um corpo se, e somente se, os únicos ideais de $A$ são os triviais ($\{0\}$ e $A$).

*Demonstração:*

($\rightarrow$) Seja $J \neq \{0\}$ um ideal em $A$. Com essa suposição, resta-nos demonstrar que $J = A$. Para isso tomemos $a \in J$, $a \neq 0$, que é inversível, por $A$ ser um corpo. A igualdade desejada, $J = A$, é então uma conseqüência da proposição 20, parte (iv).

($\leftarrow$) Temos de provar apenas que todo elemento de $A$, não nulo, é inversível. Para tanto, seja $a \in A$, $a \neq 0$, e consideremos o ideal $J = \langle a \rangle$. Como $J \neq \{0\}$, pois $a \in J$, então $J = A$ e, portanto, $1 \in J$. Dessa relação segue que $1 \quad ax_0$, para um conveniente $x_0 \in A$. De onde, $a$ é inversível. #

## 18. OPERAÇÕES COM IDEAIS

### 18.1 Interseção

Se $I$ e $J$ são ideais em $A$, então $I \cap J$ também é um ideal em $A$. De fato:

- Como $0 \in I$ e $0 \in J$, então $0 \in I \cap J$.
- Se $x, y \in I \cap J$, então $x, y \in I$ e $x, y \in J$. Segue daí que $(x - y) \in I$ e $(x - y) \in J$ e, portanto, $(x - y) \in I \cap J$.
- Sejam $x \in I \cap J$ e $a \in A$. Então $x \in I$, $x \in J$ e, portanto, $ax \in I$ e $ax \in J$. De onde, $ax \in I \cap J$.

**Proposição 22:** Se $I$ e $J$ são ideais em $A$, então $I \cap J$ é o "maior" ideal contido em $I$ e em $J$. (No enunciado, "maior" significa que todo ideal contido em $I$ e em $J$ também está contido em $I \cap J$.)

*Demonstração:* Seja $L$ um ideal em $A$ contido em $I$ e em $J$. Portanto, se $x \in L$, então $x \in I$ e $x \in J$ e, por conseguinte, $x \in I \cap J$. Se todo elemento de $L$ pertence também a $I \cap J$, então $L \subset I \cap J$. #

### 18.2 Adição

Sejam $I$ e $J$ ideais em um anel comutativo $A$. A *soma* desses ideais é o subconjunto de $A$, indicado por $I + J$, e assim definido:

$$I + J = \{x + y \mid x \in I \text{ e } y \in J\}$$

Vamos mostrar que $I + J$ também é um ideal em $A$ e, portanto, que a lei que associa a cada par de ideais de um anel sua soma é uma operação no conjunto de todos os ideais desse anel.

- Como $0 \in I$ e $0 \in J$, então $0 = 0 + 0 \in I + J$.
- Se $r, s \in I + J$, então $r = x_1 + y_1$ e $s = x_2 + y_2$, para elementos convenientes $x_1, x_2 \in I$ e $y_1, y_2 \in J$. Então $r - s = (x_1 - x_2) + (y_1 - y_2) \in I + J$, uma vez que $(x_1 - x_2) \in I$ e $(y_1 - y_2) \in J$.
- Sejam $t \in I + J$ e $a \in A$. Então $t = x + y$ ($x \in I, y \in J$) e $at = ax + ay$. Como $ax \in I$ e $ay \in J$, então $at \in I + J$.

**Proposição 23:** Se $I$ e $J$ são ideais em um anel comutativo $A$, então: (i) $I + J$ contém $I$ e $J$; (ii) $I + J$ é o "menor" ideal em $A$ com essa propriedade. (No caso, "menor" significa que todo ideal em $A$ que contém $I$ e contém $J$ também contém $I + J$.)

*Demonstração:*

(i) Seja $x \in I$. Como $x = x + 0$ e $0 \in J$, então $x \in I + J$. Esse raciocínio mostra que $I + J \supset I$. De maneira análoga se prova que $I + J \supset J$.

(ii) Seja $L$ um ideal em $A$ tal que $L \supset I$ e $L \supset J$. Devemos provar que todo elemento de $I + J$ também é elemento de $L$. De fato, se $r \in I + J$, então $r = x + y$ ($x \in I$, $y \in J$). Como $L \supset I$, então $x \in L$; e como $L \supset J$, então $y \in L$. Logo, $x + y = r \in L$. #

*Exemplo 47.* Nosso objetivo aqui é determinar a soma de dois ideais em $\mathbb{Z}$. Como todo ideal em $\mathbb{Z}$ é principal, entao devemos determinar $d$ na igualdade:

$$\langle a \rangle + \langle b \rangle = \langle d \rangle$$

dados $a, b \in \mathbb{Z}$. Observemos primeiro que, como $a = 1 \cdot a + 0 \cdot b$, então $a \in \langle a \rangle + \langle b \rangle = \langle d \rangle$. Logo, $a = td$, para algum inteiro $t$, e, portanto, $d \mid a$. Analogamente se demonstra que $d \mid b$.

Como, por outro lado, $d \in \langle a \rangle + \langle b \rangle$, então pode-se representar $d$ assim: $d = ra + sb$, em que $r, s \in \mathbb{Z}$. Dessa igualdade decorre que todo divisor de $a$ e $b$ também é divisor de $d$.

Então o inteiro $d$ goza das seguintes propriedades: (a) é divisor de $a$ e $b$; (b) todo divisor de $a$ e $b$ é também seu divisor. De onde, $d = \text{mdc}(a, b)$ ou $d = -\text{mdc}(a, b)$.

Por exemplo:

$$\langle 2 \rangle + \langle 3 \rangle = \langle 1 \rangle = \mathbb{Z}$$

pois $\text{mdc}(2, 3) = 1$.

## 19. IDEAIS PRIMOS E MAXIMAIS

**Definição 18:** Seja $P$ um ideal em um anel comutativo $A$. Diz-se que $P$ é um *ideal primo* se $P \neq A$ e se qualquer relação do tipo $ab \in P$, em que $a, b \in A$, tiver como consequência que $a \in P$ ou $b \in P$.

*Exemplo 48.* No anel $\mathbb{Z}$ o ideal $I = \{0\}$ é primo, pois, se $ab \in I$, isto é, se $ab = 0$, então $a = 0$ ou $b = 0$, ou seja, $a \in I$ ou $b \in I$. Obviamente o mesmo ocorre com um anel de integridade qualquer.

*Exemplo 49:* O ideal $2\mathbb{Z}$ é primo em $\mathbb{Z}$. De fato, se $ab \in 2\mathbb{Z}$, então $2 \mid ab$ e, portanto, como 2 é primo, $2 \mid a$ ou $2 \mid b$. De onde, $a \in 2\mathbb{Z}$ ou $b \in 2\mathbb{Z}$.

*Exemplo 50:* No anel produto direto $\mathbb{Z} \times \mathbb{Z}$ o ideal $I = \{0\} \times \mathbb{Z}$ é primo. De fato, se $(a, b), (c, d)$ são elementos de $\mathbb{Z} \times \mathbb{Z}$ tais que $(a, b)(c, d) = (ac, bd) \in \{0\} \times \mathbb{Z}$, então $ac = 0$ e, portanto, $a = 0$ ou $c = 0$. De onde, $(a, b) \in \{0\} \times \mathbb{Z}$ ou $(c, d) \in \{0\} \times \mathbb{Z}$.

**Definição 19:** Seja $P$ um ideal num anel comutativo $A$. Diz-se que $M$ é um *ideal maximal* se $M \neq A$ e se os únicos ideais em $A$ que contêm $M$ são o próprio $M$ e $A$.

*Exemplo 51:* $2\mathbb{Z}$ é um ideal maximal em $\mathbb{Z}$. De fato, se $I$ é um ideal em $\mathbb{Z}$ que contém $2\mathbb{Z}$ propriamente, então $I$ possui um número ímpar $2t + 1$. Mas, como $2t \in I$, pois $2t$ pertence a $2\mathbb{Z}$ e $I \supset 2\mathbb{Z}$, então $(2t + 1) - (2t) = 1 \in I$. De onde, $I = \mathbb{Z}$.

*Exemplo 52:* No anel produto direto $A = \mathbb{Z} \times \mathbb{Z}$ é maximal o ideal $2\mathbb{Z} \times \mathbb{Z}$. Para provar essa afirmação, seja $I$ um ideal em $A$ que contém propriamente $2\mathbb{Z} \times \mathbb{Z}$. Então $I$ possui um elemento do tipo $(2r + 1, s)$, em que $r, s \in \mathbb{Z}$. Mas, como $(2r, s - 1) \in I$, porque pertence a $2\mathbb{Z} \times \mathbb{Z}$, que é uma parte de $I$, então $(2r + 1, s) - (2r, s - 1) = (1, 1) \in I$. Como a unidade do anel pertence a $I$, então $I = \mathbb{Z} \times \mathbb{Z}$.

**Proposição 24:** Todo ideal maximal em um anel comutativo é necessariamente um ideal primo.

*Demonstração:* Seja $M$ um ideal maximal em um anel comutativo $A$. Da definição de ideal maximal decorre diretamente que $M \neq A$. Basta provar que, se $a$, $b$ são elementos de $A$ tais que $ab \in M$, então $a \in M$ ou $b \in M$. Suponhamos que $a \notin M$ e consideremos o ideal $I = \langle a \rangle + M$. Observemos que, devido à proposição 23, $I \supset M$.

Como, porém, $a \in I$, pois $a = 1 \cdot a + 0$ e $0 \in M$, e estamos supondo que $a \notin M$, então $I$ contém propriamente $M$ e, portanto, $I = A$. Isso implica que a unidade de $A$ pode ser escrita assim:

$$1 = ra + m$$

em que $r$ e $m$ são convenientes elementos de $A$ e $M$, respectivamente. Multiplicando-se os dois membros dessa igualdade por $b$:

$$b = r(ab) + bm$$

igualdade que mostra que $b \in M$, posto que tanto $ab$ como $m$ são elementos de $M$. #

*Contra exemplo 6:* O ideal $\{0\} \times \mathbb{Z}$ é primo em $\mathbb{Z} \times \mathbb{Z}$, como já mostramos (exemplo 50), mas não é maximal. De fato, é só observar que $2\mathbb{Z} \times \mathbb{Z}$ é também um ideal em $\mathbb{Z} \times \mathbb{Z}$, que $2\mathbb{Z} \times \mathbb{Z}$ contém propriamente $\{0\} \times \mathbb{Z}$ e que, obviamente, $2\mathbb{Z} \times \mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z}$.

Esse contra-exemplo mostra que a recíproca da proposição 24 não é verdadeira.

## Exercícios

**99.** Verifique se são ideais:

a) $\{\bar{0}, \bar{2}, \bar{4}\}$ no anel $\mathbb{Z}_6$;

b) $m\mathbb{Z}$ no anel $\mathbb{Z}$;

c) $m\mathbb{Z} \times n\mathbb{Z}$ no anel $\mathbb{Z} \times \mathbb{Z}$;

d) $\{x \in \mathbb{Z} \mid \text{mdc}(x, 5) = 1\}$ no anel $\mathbb{Z}$;

e) $\{x \in \mathbb{Z} \mid 25 \text{ divide } 35x\}$ no anel $\mathbb{Z}$;

f) $\{x \in \mathbb{Z} \mid x \text{ divide } 24\}$ no anel $\mathbb{Z}$;

g) $\{x \in \mathbb{Z} \mid 6 \text{ divide } x \text{ e } 24 \text{ divide } x^2\}$ no anel $\mathbb{Z}$;

h) $\mathbb{Z}$ no anel $(\mathbb{Q}, \oplus, \odot)$ em que $a \oplus b = a + b - 1$ e $a \odot b = a + b - ab$, para todo $a, b \in \mathbb{Q}$;

i) $2\mathbb{Z}$ no anel $(\mathbb{Z}, +, \cdot)$ em que a adição é a usual e $a \cdot b = 0$, para todo $a, b \in \mathbb{Z}$;

j) $\{f: \mathbb{R} \to \mathbb{R} \mid f(0) = 0\}$ no anel $\mathbb{R}^{\mathbb{R}}$.

**100.** Sendo $A$ um anel (eventualmente não comutativo), dizemos que $I \subset A$ e $I \neq \varnothing$ é um ideal à esquerda em $A$ se, e somente se:

$$(\forall x, y)(x \in I \text{ e } y \in I \Rightarrow x - y \in I) \text{ e } (\forall x, z)(x \in A \text{ e } z \in I \Rightarrow xz \in I)$$

Verifique se são ideais à esquerda em $M_2(R)$:

a) $L_1 = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$

b) $L_2 = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}\right\}$

c) $L_3 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$

d) $L_4 = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$

**101.** Mostre que é um ideal em $A$ (anel comutativo) o conjunto dos seus elementos nilpotentes. *Sugestão:* Para mostrar que esse conjunto é fechado para a subtração, tomando $x$ e $y$ nilpotentes e tais que $x^r = y^s = 0$, considere $(x - y)^{r+s}$.

**102.** Descreva os seguintes ideais principais:

a) $\langle \bar{2} \rangle$ em $\mathbb{Z}_6$

b) $\langle -5 \rangle$ em $\mathbb{Z}$

c) $\left\langle \frac{2}{7} \right\rangle$ em $\mathbb{Q}$

d) $\langle \sqrt{2} \rangle$ em $\mathbb{R}$

e) $\langle \bar{3} \rangle$ em $\mathbb{Z}_8$

f) $\langle 2 \rangle$ em $2\mathbb{Z}$

g) $\left\langle -\frac{3}{5} \right\rangle$ em $\mathbb{R}$

h) $\langle 1 - i \rangle$ em $\mathbb{C}$

**103.** Determine todos os ideais de $\mathbb{Z}_8$.

**104.** Mostre que todos os ideais de um anel $\mathbb{Z}_m$ são principais

**105.** a) Seja $I$ um ideal do anel comutativo $A$. Prove que $J = \{x \in A \mid x \cdot i = 0, \forall i \in I\}$ é um ideal de $A$.

b) Determine $J$ no caso $A = \mathbb{Z}_{16}$ e $I = \langle \bar{2} \rangle$.

**106.** Sejam $A$ um anel e $J$ um ideal à esquerda. Seja $M$ o conjunto de todos os $x \in A$ tais que $xJ = \{0\}$. Mostre que $M$ é um ideal em $A$. ($xJ = \{xj \mid j \in J\}$.)

**107.** Seja $A$ um anel comutativo. Dados $a \in A$ e $b \in A$, dizemos que "$a$ é associado de $b$" quando $a \mid b$ e $b \mid a$.

a) Prove que "$a$ é associado de $b$" equivale a "os ideais $\langle a \rangle$ e $\langle b \rangle$ são iguais".

b) Quais são os elementos associados de 5 no anel $\mathbb{Z}$?

**108.** Sejam $a$, $b$, $c$ elementos do anel de integridade $\mathbb{Z}$. Mostre que, se $a = bc$ e $b \neq \pm a$, então $\langle a \rangle \underset{\neq}{\subset} \langle b \rangle$.

**109.** Sejam $I = \langle a \rangle$ e $J = \langle b \rangle$ ideais em um anel $A$. Mostre que $I \cdot J = \{xy \mid x \in I$ e $y \in J\}$ é um ideal em $A$ e $I \cdot J = \langle ab \rangle$.

**110.** Sejam $I$ e $J$ dois ideais do anel $A$. Mostre que, se $I \cap J$ $\{0\}$, então $xy$ 0, para todo $x \in I$ e $y \in J$

**111.** Se $(I_r)$ é uma família de ideais, mostre que $\bigcap_r I_r$ é um ideal.

**112.** a) Dê um exemplo de dois ideais $I$ e $J$ em um anel $A$ de modo que $I \cup J$ não é ideal de $A$.

b) Se $I_1 \subset I_2 \subset I_3 \ldots$ é uma sequência de ideais em $A$, mostre que $\bigcup_r I_r$ é um ideal de $A$.

**113.** Seja $A$ um anel com as operações $+$ e $\cdot$.

Mostre que:

a) $A \times \mathbb{Z}$ é um anel em relação às operações $\oplus$ e $\odot$ assim definidas:

$(a, m) \oplus (b, n) = (a + b, m + n)$

$(a, m) \odot (b, n) = (ab + mb + na, mn)$

b) $A \times \{0\}$ é um ideal em $A \times \mathbb{Z}$.

c) A aplicação $f: A \to A \times \{0\}$ tal que $f(x) = (x, 0)$ é um isomorfismo.

**114.** Sejam $I = \langle x \rangle$ e $J = \langle y \rangle$ dois ideais de $\mathbb{Z}$. Mostre que $I + J = \langle \text{mdc}(x, y) \rangle$ e que $I \cap J = \langle \text{mmc}(x, y) \rangle$; em seguida determine $\langle 12 \rangle + \langle 21 \rangle$ e $\langle 12 \rangle \cap \langle 21 \rangle$.

**Resolução**

1º) Lembremos que $m$ é mmc$(a, b)$ se, e somente se, $a \mid m, b \mid m; a \mid m'$ e $b \mid m' \Rightarrow m$ $m'; m \geqslant 0$.

Provemos que $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$. Sendo $x$ um elemento qualquer de $\mathbb{Z}$, temos:

$$x \in \langle a \rangle \cap \langle b \rangle \Leftrightarrow \begin{cases} x \in \langle a \rangle \Leftrightarrow a \mid x \\ x \in \langle b \rangle \Leftrightarrow b \mid x \end{cases} \Leftrightarrow m \mid x \Leftrightarrow x \in \langle m \rangle$$

Portanto, $\langle a \rangle \cap \langle b \rangle \subsetneqq \langle m \rangle$.

2º) Lembremos que $d$ é um mdc$(a, b)$ se, e somente se, $d \geqslant 0; d \mid a, d \mid b; d' \mid a$ e $d' \mid b \Rightarrow$ $\Rightarrow d'$ $d$. Provemos que $\langle a \rangle + \langle b \rangle = \langle d \rangle$. Para qualquer inteiro $x$, temos:

$$\left.\begin{array}{l} x \in \langle a \rangle + \langle b \rangle \Rightarrow x = ra + sb \\ \qquad\qquad\qquad\quad d \mid a \\ \qquad\qquad\qquad\quad d \mid b \end{array}\right\} \Rightarrow d \mid x \Rightarrow x \in \langle d \rangle$$

Portanto, $\langle a \rangle + \langle b \rangle \subset \langle d \rangle$

Sendo $\langle a \rangle + \langle b \rangle$ um ideal em $\mathbb{Z}$, $\langle a$ $+ \langle b \rangle$ é um ideal principal Seja $d'$ um gerador de $a,$ $+$ $b \rangle$ Temos

$$\left.\begin{array}{l} a = a + 0 \Rightarrow a \in \langle a \rangle + \langle b \rangle \Rightarrow d' \mid a \\ b = 0 + b \Rightarrow b \in a \; + \langle b \rangle \Rightarrow d' \mid a \end{array}\right\} \Rightarrow d' \; d \Rightarrow \langle d \rangle \subset \langle d' \rangle$$

$\langle d \rangle \subset \langle a \rangle + \langle b$

3º Em consequência do exposto

$\langle 12$ $\cap$ $21 \rangle$ $\langle \text{mmc}(12\ 21) \rangle$ $\langle 84 \rangle$

$\langle 12 \rangle + \langle 21$ $-$ mdc$(12, 21) \rangle - \langle 3$

**115.** Sejam $a, b$ e $c$ elementos fixados de um anel $A$. Prove que $\langle a, b, c \rangle = \{ax + by + cz \mid x, y, z \in A\}$ é um ideal em $A$. Em seguida, determine $m \in \mathbb{Z}$ tal que $\langle 12, 20, 28 \rangle = \langle m \rangle$ no anel $\mathbb{Z}$.

**116.** Seja $f$ um homomorfismo do anel $A$ no anel $A'$. Mostre que, se $I$ e $J$ são ideais em $A$, então $f(I + J) = f(I) + f(J)$.

**117.** Seja $I$ um ideal no anel $A$ e $a$ um elemento fixo de $A$. Mostre que o conjunto $\langle I, a \rangle = \{i + ra \mid i \in I \text{ e } r \in A\}$ é ideal em $A$.
Determine, no caso $A = \mathbb{Z}$, o ideal $\langle \langle 4 \rangle, 6 \rangle$.

**118.** No anel $\mathbb{Z}$ considere o ideal $I = \langle 3 \rangle$. Mostre que o único ideal em $\mathbb{Z}$ que contém $I$ é o próprio $\mathbb{Z}$; generalize esse resultado.

**119.** Sejam $a_1, a_2, \ldots, a_m \in A$. Supondo $A$ um anel comutativo com unidade, mostre que $\langle a_1, a_2, \ldots, a_m \rangle$ é o menor ideal em $A$ que contém $\{a_1, a_2, \ldots, a_m\}$.

**120.** Seja $a$ um elemento idempotente de um anel $A$ comutativo com unidade. Mostre que $A = \langle a \rangle + \langle 1 - a \rangle$ e que $\langle a \rangle \cap \langle 1 - a \rangle = \{0\}$.

**121.** Mostre que um anel comutativo com unidade $A$ é anel de integridade se, e somente se, $\langle 0 \rangle$ é primo.

**122.** Dê exemplos de ideais primos e não maximais.

**123.** Seja $a \neq 0$ um número inteiro. Prove que $\langle a \rangle$ é primo se, e somente se, $a$ é primo.

**124.** Se $I$ é um ideal no anel $A$ e se $P$ é um ideal primo em $I$, então $P$ é um ideal em $A$. Prove.

**125.** Mostre que todo ideal primo $P \neq \langle 0 \rangle$ em $\mathbb{Z}$ é maximal.

**126.** Mostre que é maximal em $A = \mathbb{R}^{\mathbb{R}}$ o ideal $M = \{f \in A \mid f(1) = 0\}$.

## Exercício complementar

**C8.** Seja $A$ o subanel de $\mathbb{R}^{\mathbb{R}}$ formado pelas funções infinitamente deriváveis. Seja $J_n$ o subconjunto de $A$ constituído pelas funções $f$ tais que todas as suas derivadas, até a de ordem $n$, se anulam em 0, ou seja:

$$J_n = \{f \in A \mid D^k f(0) = 0, \forall k, 0 \leq k \leq n\}$$

Mostre que $J_n$ é um ideal de $A$.

# V-6 ANÉIS QUOCIENTES

Seja $I$ um ideal em um anel comutativo $A$. Conforme já vimos (seção 16), $I$ é um subanel de $A$ e, portanto, um subgrupo do grupo aditivo $A$. E como esse grupo é comutativo, então $I$ é um subgrupo normal de $(A, +)$. Logo, tem sentido considerar o grupo quociente $A/I$ cujos elementos são as classes laterais $a + I$ $(a \in A)$ e cuja adição é definida por $(a + I) + (b + I) = (a + b) + I$ $(a, b \in A)$. Lembremos que o elemento neutro de $A/I$ é a classe $0 + I = I$ e que o elemento oposto de uma classe $a + I$ é a classe $(-a) + I$. A proposição que segue mostra que o grupo $A/I$ pode se converter em um anel de uma maneira muito natural.

**Proposição 25:** Seja $I$ um ideal em um anel comutativo $A$. Considerando-se $I$ como subgrupo normal de $A$, então o grupo quociente $A/I$ torna-se um anel comutativo definindo-se a multiplicação em $A/I$ assim:

$$(a + I)(b + I) = (ab) + I$$

*Demonstração:* Primeiro é preciso demonstrar que essa multiplicação está bem definida, ou seja, que não depende dos elementos de $A$ usados na representação das classes. Para isso, suponhamos $a_1 + I = a_2 + I$ e $b_1 + I = b_2 + I$ e mostremos que

$$a_1b_1 + I = a_2b_2 + I$$

De $a_1 + I = a_2 + I$ segue que $a_1 - a_2 \in I$ e, analogamente, de $b_1 + I = b_2 + I$ segue que $b_1 - b_2 \in I$. Portanto, levando-se em conta que $I$ é um ideal em $A$:

$$b_1(a_1 - a_2) \in I \text{ e } a_2(b_1 - b_2) \in I$$

Logo:

$$[b_1(a_1 - a_2) + a_2(b_1 - b_2)] = (a_1b_1 - a_2b_2) \in I.$$

Isso significa que $a_1b_1 + I = a_2b_2 + I$, como queríamos mostrar.

Falta provar as propriedades da multiplicação necessárias para completar a estrutura de anel comutativo em $A/I$. Dado que o raciocínio é o mesmo sempre, nos ateremos a demonstrar a distributividade da multiplicação em relação à adição. Para isso, sejam $a, b, c \in A$. Então:

$$(a + I)[(b + I) + (c + I)] = (a + I)[(b + c) + I] = [a(b + c)] + I = (ab + ac) + I =$$

$$= (ab + I) + (ac + I) = (a + I)(b + I) + (a + I)(c + I) \ \#$$

*Contra exemplo 7:* Se $A$ possui unidade e $J$ é um ideal em $A$, então o anel quociente $A/J$ também possui é a classe $1 + J$ ($1 =$ unidade de $A$). De fato, $(a + J)(1 + J) = a \cdot 1 + J = a + J$.

Mas $A/J$ não é necessariamente um anel de integridade quando $A$ é um anel de integridade. Para mostrar isso, consideremos o anel de integridade $\mathbb{Z}$ e o ideal $J = \langle 6 \rangle$ nesse anel. As classes $2 + J$ e $3 + J$ são diferentes do zero do anel quociente, que é a classe $0 + J = J$. De fato, se, por exemplo, $2 + J = J$, então $2 \in J$,

o que nao ocorre. No entanto, $(2 + J)(3 + J) = 6 + J = J$, uma vez que $6 \in J$. Ou seja, $2 + J$ e $3 + J$ são divisores próprios do zero em $\mathbb{Z}/J$.

**Proposição 26:** Sejam $A$ um anel de comutativo com unidade e $J$ um ideal em $A$. Então: (i) $J$ é um ideal primo se, e somente se, $A/J$ é um anel de integridade; (ii) $J$ é um ideal maximal se, e somente se, $A/J$ é um corpo.

*Demonstração:*

(i)

$(\rightarrow)$ Basta provar que $A/J$ não possui divisores próprios do zero. Para isso, sejam $a + J, b + J \in A/J$. Se $(a + J)(b + J) = ab + J = J$ (zero do anel quociente), então $ab \in J$ e, como $J$ é primo, então $a \in J$ ou $b \in J$. Mas isso significa que $a + J = J$ ou $b + J = J$ (zero do anel quociente $A/J$). Portanto, $A/J$ não possui divisores próprios do zero, como queríamos demonstrar.

$(\leftarrow)$ Sejam $a, b \in A$ tais que $ab \in J$. Então $ab + J = (a + J)(b + J) = J$ (zero de $A/J$). Mas, como $A/J$ é, por hipótese, um anel de integridade e, portanto, não possui divisores próprios do zero, então $a + J = J$ ou $b + J = J$, ou seja, $a \in J$ ou $b \in J$. Portanto, $J$ é um ideal primo.

(ii)

$(\rightarrow)$ Basta provar que todo elemento $a + J \neq J$ é inversível. Dessa desigualdade segue que $a \notin J$ e, portanto, $\langle a \rangle + J = A$. Então a unidade de $A$ pode ser escrita assim: $1 = ab + m$, para algum $b \in A$ e algum $m \in J$. Daí, $1 - ab = m \in J$ e, portanto:

$$1 + J = (ab) + J = (a + J)(b + J)$$

o que mostra que $b + J$ é o inverso de $a + J$ no anel quociente $A/J$.

$(\leftarrow)$ Sendo $A/J$ um corpo, então $J \neq A$. De fato, se $J = A$, então $A/J = \{J\}$, e isso é incompatível com a hipótese de $A/J$ ser um corpo. Falta provar que o único ideal que contém $J$ propriamente é $A$. Para tanto, denotemos por $K$ um ideal em $A$ tal que $K \supset J$ e $K \neq J$ e consideremos um elemento $a \in K - J$. Como $a \notin J$, então $a + J \neq J$, ou seja, $a + J$ é um elemento não nulo de $A/J$ e, portanto, tem um inverso $b + J$ no anel. Daí, $(a + J)(b + J) = 1 + J$, igualdade que tem como conseqüência que $ab - 1 \in J$. Logo, $ab - 1 \in K$ e, como $a \in K$, então $1 \in K$. Dessa relação segue que $K = A$. Ou seja, o único ideal que contém $J$ propriamente é $A$ e, portanto, $J$ é maximal. #

**Proposição 27:** Seja $I$ um ideal em um anel comutativo $A$ e consideremos a aplicação $\mu: A \rightarrow A/I$ assim definida: $\mu(a) = a + I$, para cada $a \in A$. Então $\mu$ é um homomorfismo sobrejetor de anéis cujo núcleo é $I$.

*Demonstração:*

Se $a, b \in A$, então:

- $\mu(a + b) = (a + b) + I = (a + I) + (b + I) = \mu(a) + \mu(b)$;
- $\mu(ab) = (ab) + I = (a + I)(b + I) = \mu(a)\,\mu(b)$.

o que demonstra que $\mu$ é um homomorfismo.

Ademais, se $y \in A/I$ então $y = a + I$, para algum $a \in A$. Tomando-se $x = a$, então $\mu(x) = \mu(a) = a + I = y$. Com isso fica demonstrado que $\mu$ é sobrejetora.

Por outro lado, se $a \in A$, então:

$a \in Ker(f)$ se, e somente se, $\mu(a) = a + I = I$,

se, e somente se, $a \in I$.

De onde, $Ker(f) = I$, como queríamos provar. #

**Definição 20:** Seja $I$ um ideal em um anel comutativo $A$. Então o homomorfismo $\mu: A \to A/I$ introduzido na proposição anterior e definido por $\mu(a) = a + I$, para cada $a \in A$, é chamado *homomorfismo canônico* de $A$ sobre $A/I$

**Proposição 28** (teorema do homomorfismo para anéis): Seja $f: A \to B$ um homomorfismo sobrejetor de anéis. Se $I = Ker(f)$, então o anel quociente $A/I$ é isomorfo a $B$.

*Demonstração:* O primeiro passo é descobrir um isomorfismo, digamos, de $A/I$ em $B$. Como um elemento genérico de $A/I$ é do tipo $a + I$ ($a \in A$) e um elemento genérico de B do tipo $f(a)(a \in A)$, pois $f$ é sobrejetor, o bom senso recomenda que se experimente a correspondência

$$a + I \to f(a).$$

E trata-se efetivamente de uma aplicação, inclusive injetora, pois:

$a + I = b + I$ se, e somente se, $a - b \in I$;

se, e somente se, $f(a - b) = 0$ (zero de $B$);

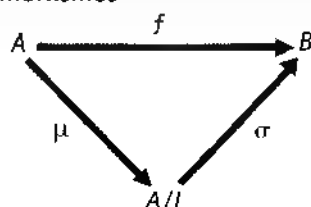
se, e somente se, $f(a) - f(b) = 0$;

se, e somente se, $f(a) = f(b)$.

Chamando-se essa aplicação de $\sigma$, então, para qualquer $a \in A, \sigma(a + I) = f(a)$. Mostremos agora que $\sigma$ é um homomorfismo de anéis.

- $\sigma((a + I) + (b + I)) = \sigma((a + b) + I) = f(a + b) = f(a) + f(b) = \sigma(a + I) + \sigma(b + I)$;
- $\sigma((a + I)(b + I)) = \sigma((ab) + I) = f(ab) = f(a)f(b) = \sigma(a + I)\sigma(b + I)$.

Deixamos como exercício a demonstração de que $\sigma$ é sobrejetora. #

Seja $f: A \to B$ um homomorfismo sobrejetor de anéis e denotemos por $I$ o núcleo de $f$. Consideremos ainda o anel quociente $A/I$, o homomorfismo canônico $\mu: A \to A/I$ e o homomorfismo $\sigma: A/I \to B$, introduzido na proposição anterior. O diagrama de anéis e homomorfismos

sugere a possibilidade de uma fatoração de $f$ através de $A/I$. Efetivamente isso ocorre, pois, para qualquer $a \in A$:

$$(\sigma \circ \mu)(a) = \sigma(\mu(a)) = \sigma(a + I) = f(a)$$

e, portanto,

$$f = \sigma \circ \mu$$

*Exemplo 53.* Consideremos um inteiro $m > 1$. Como já vimos (exemplo 25), a aplicação $p_m: \mathbb{Z} \to \mathbb{Z}_m$ definida por $p_m(r) = \overline{r}$, para cada $r \in \mathbb{Z}$, é um homomofismo sobrejetor de anéis. Vimos também (exemplo 29) que $N(p_m) = \{0, \pm m, \pm 2m, ...\} = \langle m \rangle$. Portanto, $\mathbb{Z}/\langle m \rangle \approx \mathbb{Z}_m$.

*Exemplo 54:* Consideremos a correspondência $\mathbb{Z}_{12} \to \mathbb{Z}_4$ definida como: $\overset{12}{\overline{a}} \to \overset{4}{\overline{a}}$, em que $\overset{12}{\overline{a}}$ e $\overset{4}{\overline{a}}$ são, respectivamente, as classes de restos módulo 12 e 4, determinada por $a \in \mathbb{Z}$. Essa correspondência pode ser assim visualizada:

$$\begin{array}{lll}
\overset{12}{\overline{0}} \to \overset{4}{\overline{0}} & \overset{12}{\overline{4}} \to \overset{4}{\overline{4}} = \overset{4}{\overline{0}} & \overset{12}{\overline{8}} \to \overset{4}{\overline{8}} = \overset{4}{\overline{0}} \\
\overset{12}{\overline{1}} \to \overset{4}{\overline{1}} & \overset{12}{\overline{5}} \to \overset{4}{\overline{5}} = \overset{4}{\overline{1}} & \overset{12}{\overline{9}} \to \overset{4}{\overline{9}} = \overset{4}{\overline{1}} \\
\overset{12}{\overline{2}} \to \overset{4}{\overline{2}} & \overset{12}{\overline{6}} \to \overset{4}{\overline{6}} = \overset{4}{\overline{2}} & \overset{12}{\overline{10}} \to \overset{4}{\overline{10}} = \overset{4}{\overline{2}} \\
\overset{12}{\overline{3}} \to \overset{4}{\overline{3}} & \overset{12}{\overline{7}} \to \overset{4}{\overline{7}} = \overset{4}{\overline{3}} & \overset{12}{\overline{11}} \to \overset{4}{\overline{11}} = \overset{4}{\overline{3}}
\end{array}$$

Mostraremos que essa correspondência, na verdade, é um homomorfismo sobrejetor de anéis, que seu núcleo é $I = \langle \overset{12}{\overline{4}} \rangle$ e que, portanto, $\mathbb{Z}_{12}/I$ é isomorfo a $\mathbb{Z}_4$.

Primeiramente mostremos que a correspondência dada é uma aplicação. De fato, se $\overset{12}{\overline{a}} = \overset{12}{\overline{b}}$, então $12 \mid (a - b)$ e, portanto, $4 \mid (a - b)$; logo, $\overset{4}{\overline{a}} = \overset{4}{\overline{b}}$. Seja $f$ o nome dessa aplicação. Então:

- $f(\overset{12}{\overline{a}} + \overset{12}{\overline{b}}) = f(\overset{12}{\overline{a + b}}) = \overset{4}{\overline{a + b}} = \overset{4}{\overline{a}} + \overset{4}{\overline{b}} = f(\overset{12}{\overline{a}}) + f(\overset{12}{\overline{b}})$;
- $f(\overset{12}{\overline{a}}\,\overset{12}{\overline{b}}) = f(\overset{12}{\overline{ab}}) = \overset{4}{\overline{ab}} = \overset{4}{\overline{a}}\,\overset{4}{\overline{b}} = f(\overset{12}{\overline{a}})\,f(\overset{12}{\overline{b}})$;
- $f$ é sobrejetora pela própria maneira como é definida.

Então $f$ é um homomorfismo sobrejetor de anéis

Por outro lado, $\overset{12}{\overline{a}} \in Ker(f)$ se, e somente se, $\overset{4}{\overline{a}} = \overset{4}{\overline{0}}$;

se, e somente se, $4 \mid a$.

Portanto, $I = Ker(f) = \{\overset{12}{\overline{0}}, \overset{12}{\overline{4}}, \overset{12}{\overline{8}}\} = \langle \overset{12}{\overline{4}} \rangle$. De onde, $\mathbb{Z}_{12}/I \approx \mathbb{Z}_4$, como queríamos mostrar.

## Exercícios

**127.** Construa as tábuas do anel quociente $A/I$ nos seguintes casos.

a) $A = \mathbb{Z}$ e $I = \langle 2 \rangle$

b) $A = \mathbb{Z}$ e $I = \langle 4 \rangle$

c) $A = \mathbb{Z}$ e $I = \langle m \rangle$

d) $A$ é um anel qualquer e $I = \langle 0 \rangle$

e) $A$ é um anel qualquer e $I = A$

f) $A = \mathbb{Z}_2 \times \mathbb{Z}$ e $I = \mathbb{Z}_2 \times 2\mathbb{Z}$

g) $A = \mathbb{Z}_6$ e $I = \langle \bar{2} \rangle$

h) $A = \mathbb{Z}_8$ e $I = N(A)$ = conjuntos dos elementos nilpotentes de $A$

**128.** Construa as tábuas dos seguintes anéis quocientes: $\mathbb{Z}_6/\langle \bar{3} \rangle$ e $(\mathbb{Z}_2 \times \mathbb{Z}_3)/\langle \bar{1}, \bar{0} \rangle$.

**129.** Prove que $2\mathbb{Z} \times 3\mathbb{Z}$ é um ideal em $\mathbb{Z} \times \mathbb{Z}$. Determine: $(\mathbb{Z} \times \mathbb{Z})/(2\mathbb{Z} \times 3\mathbb{Z})$.

**130.** Quais são os possíveis anéis quocientes no corpo $\mathbb{R}$ dos números reais?
*Sugestão:* Lembrar da proposição 21

**131.** Mostre que, se $A$ possui unidade, então $A/I$ também possui.

**132.** Mostre que $a + I \in A/I$ é inversível (supondo $A$ com unidade) se, e somente se, $\exists r \in A$ de modo que $a \cdot r = 1 \in I$

**Resolução**

($\Rightarrow$) Suponhamos que o inverso de $a + I$ seja $r + I$ Então, $(a + I)(r + I) = 1 + I$; daí $ar + I = 1 + I$ e, portanto, $ar - 1 \in I$.

($\Leftarrow$) Se existe $r \in A$ tal que $ar - 1 \in I$, então $ar + I = (a + I)(r + I) = 1 + I$ e $a + I$ é inversível. ∎

**133.** Dê um exemplo de anel de integridade $A$ e de ideal $I$ em $A$ tal que $A/I$ não é de integridade.
Resolva o mesmo exercício quando $A$ é um corpo.

**134.** Sendo $I$ o ideal constituído pelos elementos nilpotentes de um anel $A$, mostre que $I$ é o único elemento nilpotente de $A/I$.

**Resolução**

Seja $a = a + I$ um elemento nilpotente de $A/I$. Temos:

$\exists n \in \mathbb{N} \; (a)^n = 0 \Rightarrow a^n = 0 \Rightarrow a^n \in I \Rightarrow \exists m \in \mathbb{N} \mid (a^n)^m = 0 \Rightarrow a^{nm} = 0 \Rightarrow$
$\Rightarrow a \in I \Rightarrow a = a + I = I$ ∎

**135.** Dado o homomorfismo $f: \mathbb{Z} \to \mathbb{Z}_4$ definido por $f(m) = \hat{m}$:

a) construa o núcleo de $f$;

b) determine o homomorfismo canônico de $\mathbb{Z}$ em $\mathbb{Z}/N(f)$.

**136.** Seja $A$ um anel comutativo e $n$, $n > 0$, um número natural dado

a) Prove $K_n = \{n \cdot a \mid a \in A\}$ é um ideal em $A$.

b) Prove que a característica de $A/K_n$ divide $n$.

**137.** Seja $S$ um conjunto não vazio e $A$ um anel comutativo.

a) Mostre que $A^S = \{f \mid f: S \to A\}$ é um anel comutativo para as operações definidas por $(f + g)(x) = f(x) + g(x)$ e $(fg)(x) = f(x)g(x)$, $\forall f, g \in A^S$ e $\forall x \in S$.

b) Para um elemento $s \in S$, seja $I_s = \{f \in A^S \mid f(s) = 0\}$, mostre que $I_s$ é um ideal maximal em $A^S$.

*Nota:* O anel $A^S$ é chamado *anel das funções de S em A*.

**138.** Seja $I$ um ideal em um anel comutativo $A$. Mostre que $A/I$ tem unidade se, e somente se, existe $e \in A$ tal que $ae - a \in I$, qualquer que seja $a \in A$.

**Exercício complementar**

**C9.** Seja $A$ um anel. Sejam $I$ e $J$ ideais em $A$ tais que $J \subset I$. Mostre que existe um homomorfismo de anéis $f: A/J \to A/I$ que leva $a + J$ em $a + I$, $a \in A$.

# V-7 ORDEM EM UM ANEL DE INTEGRIDADE

## 20. ANÉIS DE INTEGRIDADE ORDENADOS

A relação de ordem usual no conjunto $\mathbb{Z}$ dos inteiros é "compatível" com as operações de $\mathbb{Z}$ no sentido de que são verdadeiras as propriedades "se $a \leqslant b$, então $a + c \leqslant b + c$" e "se $a \leqslant b$ e $c \geqslant 0$, então $ac \leqslant bc$". Essa compatibilidade não ocorre, por exemplo, quando se considera $\mathbb{Z}$ ordenado pela relação de divisibilidade. De fato, embora se verifique no que se refere à multiplicação, o mesmo não acontece quanto à adição, pois, por exemplo, 3 divide 6, mas $3 + 2 = 5$ não divide $6 + 2 = 8$. A definição que segue tem por objetivo postular as condições que devem caracterizar a "compatibilidade" de uma relação de ordem com as operações de um anel.

**Definição 21:** Consideremos um par ordenado constituído de um anel de integridade $(A, +, \cdot)$ e uma relação de ordem total $\leqslant$ sobre $A$. Nessas condições, diz-se que $(A, +, \cdot, \leqslant)$ é um *anel de integridade ordenado* quando os seguintes axiomas se cumprem:

$(O_1)$ Quaisquer que sejam $a, b, c \in A$, se $a \leqslant b$, então $a + c \leqslant b + c$.

$(O_2)$ Quaisquer que sejam $a, b, c \in A$, se $a \leqslant b$ e $0 \leqslant c$, então $ac \leqslant bc$.

• Em várias proposições a serem demonstradas, a hipótese de que $A$ é um anel de integridade poderia ser substituída por uma mais geral (anel comutativo com unidade, por exemplo). Mas, visando às situaçoes mais importantes, e para não picar muito o raciocínio, as proposições serão sempre enunciadas para anéis de integridade.

• Os axiomas $O_1$ e $O_2$ caracterizam, respectivamente, o que se entende por *compatibilidade da relação de ordem com a adição e com a multiplicação.*

• Vale observar ainda que, embora, pela definição dada, um anel de integridade ordenado seja um sistema $(A, +, \cdot, \leqslant)$, que obedece às imposições da definição 21, muitas vezes, subentendidas as operações e a relação de ordem, e para simplificar a linguagem, usaremos expressões como "o anel de integridade ordenado $A$", "seja $A$ um anel de integridade ordenado", ou mesmo, apenas, "anel ordenado" para designar esse novo objeto matemático.

*Exemplo 55:* Os anéis de integridade $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são anéis de integridade ordenados no que se refere à ordem usual $\leqslant$.

## 21. PROPRIEDADES IMEDIATAS DE UM ANEL DE INTEGRIDADE ORDENADO

Nas considerações que seguem usaremos, como é praxe, as seguintes notações:

$a \geqslant b$ para indicar que $b \leqslant a$;

$a < b$ para indicar que $a \leqslant b$ e $a \neq b$;

$a > b$ para indicar que $b < a$.

**Proposição 29:** Em um anel ordenado (ou seja, anel de integridade ordenado), são equivalentes as afirmações: (i) $a \leqslant b$; (ii) $a - b \leqslant 0$; (iii) $-b \leqslant -a$.

*Demonstração.*

(i) → (ii) Devido a $(O_1)$, de $a \leqslant b$ segue que $a + (-b) \leqslant b + (-b)$. Portanto, $a - b \leqslant 0$.

(ii) → (iii) Por hipótese $a - b \leqslant 0$. Dessa relação segue, devido a $(O_1)$, que $(a - b) + (-a) \leqslant 0 + (-a)$. De onde, $-b \leqslant -a$.

(iii) → (i) Para a demonstração, neste caso, é só somar $(a + b)$ a cada um dos membros de $-b \leqslant -a$, o que é permitido, mais uma vez, por $(O_1)$. #

**Proposição 30:** Seja $A$ um anel ordenado. Então, para quaisquer $a, b, c \in A$:

(i) Se $a + c \leq b + c$, então $a \leq b$.

(ii) $a < b$ se, e somente se, $a + c < b + c$.

*Demonstração.*

(i) Da hipótese, $a + c \leq b + c$, segue, devido a $(O_1)$, que $(a + c) + (-c) \leq (b + c) + (-c)$. Então $a + [c + (-c)] \leq b + [c + (-c)]$ e, portanto, $a + 0 \leq b + 0$. De onde, $a \leq b$.

(ii)

$(\rightarrow)$ Por hipótese, $a < b$, ou seja, $a \leq b$ e $a \neq b$. Então, devido ao axioma $(O_1)$, $a + c \leq b + c$. Como não se pode ter $a + c = b + c$, pois isso acarretaria $a = b$, então $a + c < b + c$.

$(\leftarrow)$ Por hipótese, $a + c < b + c$. Então $a + c \leq b + c$ e $a + c \neq b + c$. Mas de $a + c \leq b + c$ decorre, como vimos em (i), que $a \leq b$. Como não se pode ter $a = b$, pois essa igualdade acarretaria $a + c = b + c$, o que contraria a hipótese, então $a < b$. #

**Corolário:** Num anel ordenado, são equivalentes as afirmações: (i) $a < b$; (ii) $a - b < 0$; (iii) $-b < -a$. Em particular são equivalentes as condições: (a) $0 < a$; (b) $-a < 0$.

A demonstração será deixada como exercício. O raciocínio é o mesmo usado na demonstração da proposição 29, o que é lícito fazer devido à parte (ii) da proposição anterior. #

**Proposição 31:** Sejam $a, b, c$ elementos de um anel ordenado. Então: $a < c$ sempre que (i) $a \leq b$ e $b < c$, (ii) $a < b$ e $b \leq c$ ou (iii) $a < b$ e $b < c$.

*Demonstração:* Demonstraremos essa proposição apenas no caso da hipótese (iii). Nos demais casos, a demonstração é análoga.

Por hipótese, $a \leq b$, $a \neq b$ e $b \leq c$, $b \neq c$. Então, devido à transitividade da relação de ordem: $a \leq c$. Suponhamos que se pudesse ter $a = c$. Então $c \leq b$ e $b \leq c$ e, portanto, como a relação de ordem goza da propriedade anti-simétrica, $b = c$, o que é absurdo. Logo, $a \leq c$ e $a \neq c$, ou seja, $a < c$. #

*Exemplo 56:* Mostrar que em um anel ordenado $A$ não pode ocorrer nenhuma das seguintes situações: (a) $a_1 \leq b_1$ e $b_1 < a_1$; (b) $a_1 < b_1$ e $b_1 \leq a_1$.

De fato, tanto no primeiro caso como no segundo teríamos, como conseqüência, que $a_1 < a_1$, o que é impossível.

**Proposição 32:** ("adição de desigualdades"): Seja $A$ um anel ordenado. Se $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in A$ e $a_i \leq b_i$ $(i = 1, 2, ..., n;\ n \geq 1)$, então

$$a_1 + a_2 + ... + a_n \leq b_1 + b_2 + ... + b_n$$

Se, ademais, $a_r < b_r$, para algum índice $r$ $(1 \leq r \leq n)$, então

$$a_1 + a_2 + ... + a_n < b_1 + b_2 + ... + b_n$$

Em particular, se $a \leqslant b$ ($a < b$) e $n$ é um inteiro $\geqslant 1$, então $n \cdot a \leqslant n \cdot b$ ($n \cdot a < < n \cdot b$)

*Demonstração:* Faremos a demonstração para $n = 2$. No caso geral, procede-se por indução sobre $n$, estendendo-se o raciocínio que será feito aqui.

Por hipótese, $a_1 \leqslant b_1$ e $a_2 \leqslant b_2$. Somando-se $a_2$ aos dois membros de $a_1 \leqslant b_1$ e $b_1$ aos dois membros de $a_2 \leqslant b_2$, o que é permitido por $(O_1)$, obtêm-se as desigualdades $a_1 + a_2 \leqslant b_1 + a_2$ e $a_2 + b_1 \leqslant b_1 + b_2$. Então, devido à transitividade da relação de ordem: $a_1 + a_2 \leqslant b_1 + b_2$.

Suponhamos que, por exemplo, $a_1 \leqslant b_1$ e $a_2 < b_2$. Então, devido ao resultado que acabamos de demonstrar, válido neste caso, pois $a_2 \leqslant b_2$ e $a_2 \neq b_2$: $a_1 + a_2 \leqslant \leqslant b_1 + b_2$. Mas de $a_2 < b_2$ decorre que $a_1 + a_2 < a_1 + b_2$. Assim, se $a_1 + a_2 = = b_1 + b_2$, então $b_1 + b_2 < a_1 + b_2$ e, portanto, $b_1 < a_1$, o que não é possível, pois, por hipótese, $a_1 \leqslant b_1$. Logo, $a_1 + a_2 \neq b_1 + b_2$ e, por conseqüência, $a_1 + a_2 < < b_1 + b_2$. #

**Proposição 33:** Se $a < b$ e $0 \leqslant c$, então $ac \leqslant bc$. Mais: $ac = bc$ se, e somente se, $c = 0$ e, portanto, $ac < bc$, sempre que $c > 0$.

*Demonstração:* Como $a < b$, então $a \leqslant b$. O axioma $(O_2)$ garante então que $ac \leqslant bc$.

Suponhamos $ac = bc$. Então $ac - bc = 0$ e, portanto, $(a - b)c = 0$. Como estamos num anel de integridade e $a \neq b$, então $c = 0$. Por outro lado, é imediato que, se $c = 0$, então, $ac = bc$. #

**Corolário:** Se $a < b$ e $c \leqslant 0$, então $bc \leqslant ac$. Mais: $ac = bc$ se, e somente se, $c = 0$ e, portanto, $bc < ac$ sempre que $c < 0$.

*Demonstração:* Como $c \leqslant 0$, então $0 \leqslant -c$. A proposição anterior garante então que $a(-c) \leqslant b(-c)$, ou seja, que $-(ac) \leqslant -(bc)$. Mas então, em virtude da proposição 29, $bc \leqslant ac$. Para justificar a segunda parte, o raciocínio é análogo ao usado na demonstração anterior. #

**Proposição 34** (regra de sinais): Num anel ordenado, $ab > 0$ se, e somente se, $a > 0$ e $b > 0$ ou $a < 0$ e $b < 0$. (Isto é, $ab > 0$ se, e somente se, $a$ e $b$ têm o "mesmo sinal".)

*Demonstração:*

($\rightarrow$) Da hipótese, $ab > 0$, decorre que $ab \neq 0$ e, portanto, $a \neq 0$ e $b \neq 0$. Suponhamos, por redução ao absurdo, que $a > 0$ e $b < 0$, ou seja, que $a$ e $b$ tivessem "sinais contrários". Então $-b > 0$ e, portanto, $a(-b) > 0 \cdot (-b)$. Mas dessa desigualdade decorre que $-(ab) > 0$. Adicionando-se essa última desigualdade com $ab > 0$ (hipótese), obtém-se $ab + [-(ab)] > 0$ ou $0 > 0$, o que é impossível. De maneira análoga se mostra a impossibilidade de $a < 0$ e $b > 0$. Então $a$ e $b$ têm o mesmo sinal sempre que $ab > 0$, como queríamos provar.

($\leftarrow$) Faremos a demonstração apenas para o caso em que $a < 0$ e $b < 0$. Dessa hipótese segue que $0 < -a$ e $0 < -b$. Então, devido à proposição 33, $(-b) \cdot 0 < (-a)(-b)$, ou seja, $0 < ab$ ou $ab > 0$. #

**Proposição 35:** $a^2 \geqslant 0$ e $a^2 = 0$ se, e somente se, $a = 0$. (Portanto, $a^2 > 0$ se $a \neq 0$.)

*Demonstração:* Como $A$ é totalmente ordenado, então $0 \leqslant a$ ou $a \leqslant 0$. No primeiro caso, multiplicando-se ambos os membros da primeira dessas desigualdades por $a$, o que é permitido por $(O_2)$, obtém-se $0 \cdot a \leqslant aa$, ou seja, $0 \leqslant a^2$. De onde, $a^2 \geqslant 0$. No segundo caso, os dois membros da segunda desigualdade podem ser multiplicados por $-a \geqslant 0$, com o seguinte resultado: $a(-a) \leqslant 0 \cdot (-a)$. Daí, $-a^2 \leqslant 0$ e, portanto, $a^2 \geqslant 0$.

Se $a^2 = aa = 0$, então $a = 0$, porque estamos num anel de integridade. Por outro lado, é óbvio que, se $a = 0$, então $a^2 = 0$. #

**Corolário 1:** Se 1 indica a unidade de um anel ordenado $A$ e 0 o zero desse anel, então $1 > 0$.

*Demonstração:* Como $1 = 1 \cdot 1 = 1^2$, então $1 \geqslant 0$. Mas, como $1 \neq 0$, então $1 > 0$. #

**Corolário 2:** Seja $A$ um anel ordenado. Se $a_1, a_2, ..., a_n \in A$, então $a_1{}^2 + a_2{}^2 + ... + a_n{}^2 \geqslant 0$. E se $a_r \neq 0$, para algum índice $r$ $(1 \leqslant r \leqslant n)$, então $a_1{}^2 + a_2{}^2 + ... + a_n{}^2 > 0$.

A proposição 35 garante que: $a_1{}^2 \geqslant 0, a_2{}^2 \geqslant 0, ..., a_n{}^2 \geqslant 0$. Isso posto, a proposição 32 garante que $a_1{}^2 + a_2{}^2 + ... + a_n{}^2 \geqslant 0$. Se $a_r \neq 0$, então $a_r{}^2 > 0$, devido à proposição anterior. Mas, neste caso, ainda devido à proposição 32, $a_1{}^2 + a_2{}^2 + ... + a_n{}^2 > 0$. #

*Exemplo 57:* O conjunto dos elementos de um anel de integridade ordenado $A$ não tem mínimo. Suponhamos que $A$ possuísse mínimo e o indiquemos por $m_o$. Lembremos que esse elemento teria de gozar da seguinte propriedade: $m_o \in A$ e $m_o \leqslant x$, qualquer que seja $x \in A$. Como, porém, $0 < 1$, então, somando-se $m_o - 1$ a ambos os membros dessa desigualdade:

$$m_o - 1 < (m_o - 1) + 1$$

Logo, $m_o - 1 < m_o$, o que é contraditório, pois $(m_o - 1) \in A$.

**Proposição 36:** A característica de um anel de integridade ordenado é zero.

*Demonstração:* Seja $A$ o anel. Então, como já vimos, $1_A > 0_A$. A proposição 32 aplicada a essa desigualdade, considerada duas vezes, leva a

$$1_A + 1_A > 0_A + 0_A$$

ou $2 \cdot 1_A > 0_A$. A aplicação de novo da proposição citada, agora para esta última desigualdade e para $1_A > 0_A$, leva a

$$3 \cdot 1_A > 0_A$$

E assim por diante. Portanto, qualquer que seja o inteiro $n > 0$

$$n \cdot 1_A > 0_A$$

Então $n \cdot 1_A \neq 0_A$, se $n > 0$, o que tem como consequência que $c(A) = 0$, como queríamos provar. #

**Corolário:** Se $(A, +, \cdot)$ é um anel de integridade finito, então nenhuma relação de ordem sobre $A$ é compatível com as operações do anel. Em outras palavras, não há como ordenar o anel $A$.

A demonstração é imediata. É só lembrar que a característica de um anel finito é maior que zero. #

## 22. ANÉIS DE INTEGRIDADE BEM ORDENADOS

**Definição 22:** Seja $A$ um anel de integridade ordenado. Então os elementos de $P = \{x \in A \mid x \geqslant 0\}$ são chamados *elementos positivos* do anel. Se todo subconjunto de $P$ (com a relação de ordem induzida pela de $A$) possui mínimo, então se diz que $A$ é um *anel de integridade bem ordenado* ou, para simplificar, *anel bem ordenado*.

*Exemplo 58.* O anel $\mathbb{Z}$ dos números inteiros é bem ordenado como nos assegura o princípio do menor número inteiro.

*Contra-exemplo 8:* O anel dos números reais, com a ordem usual, não é bem ordenado. De fato, qualquer que seja $a \in I = ]0, 1]$, $a/2 \in I$ e $a/2 < a$

**Proposição 37:** Seja $A$ um anel bem ordenado. Então $A$ não possui nenhum elemento $x$ tal que $0 < x < 1$.

*Demonstração.* Se o conjunto $L = \{x \in A \mid 0 < x < 1\}$ não fosse vazio, então possuiria mínimo, pois $L \subset P$. Se $a$ indica esse mínimo, então $0 < a < 1$. Multiplicando-se os termos dessas desigualdades por $a$:

$$0 < a^2 < a$$

Como $a < 1$, então:

$$0 < a^2 < a < 1$$

Essas relações mostram que $a^2 \in L$ e $a^2 < a$, o que é absurdo. #

**Definição 23:** Um anel de integridade ordenado $A$ se diz *arquimediano* se, qualquer que seja $a \in A$, existe um número natural $n > 0$ tal que $n \cdot 1_A > a$.

**Proposição 38:** Todo anel de integridade bem ordenado é arquimediano.

*Demonstração:* Suponhamos que um anel bem ordenado $A$ não fosse arquimediano. Então, para algum $a \in A$, $n \cdot 1_A \leqslant a$, não importa qual o número natural $n > 0$. Seja $L = \{a - n \cdot 1_A \mid n \in \mathbb{N}^*\}$. Devido à suposição feita, todo elemento de $L$ é positivo, e como $A$ é bem ordenado, $L$ possui um mínimo. Seja $a - r \cdot 1_A$ esse

mínimo e observemos o elemento $a - (r + 1) \cdot 1_A$, que também pertence a $L$. Como $1_A > 0_A$, então $r \cdot 1_A + 1_A > r \cdot 1_A + 0_A$, ou seja, $(r + 1) \cdot 1_A > r \cdot 1_A$. Daí, $-(r + 1) \cdot 1_A < -r \cdot 1_A$ e, portanto, $a + [-(r + 1) \cdot 1_A] < a + [-(r \cdot 1_A)]$. Transformando-se as adições em subtrações, chega-se a $a - (r + 1) \cdot 1_A < a - r \cdot 1_A$, o que é impossível, uma vez que $a - (r + 1) \cdot 1_A \in L$ e $a - r \cdot 1_A$ é o mínimo de $L$. Isso prova que $A$ é arquimediano. #

*Contra-exemplo 9:* Um anel pode ser arquimediano sem ser bem ordenado. É o caso, por exemplo, do anel $\mathbb{R}$ dos números reais, pelo fato de que $n \cdot 1 = n$ e de que sempre há um número natural maior que qualquer número real dado.

## 23. CORPOS ORDENADOS

Seja $K$ um corpo. Então $K$ é um anel de integridade e, como tal, pode se tratar de um anel ordenado. Neste caso, diz-se que $K$ é um *corpo ordenado*.

*Exemplo 59:* Os corpos $\mathbb{Q}$ e $\mathbb{R}$ são corpos ordenados, como já observamos anteriormente.

*Contra-exemplo 10.* Mostraremos a seguir que não há nenhuma relação de ordem total sobre $\mathbb{C}$ compatível com as operações que transformam esse conjunto no corpo dos números complexos.

De fato, suponhamos que $\mathbb{C}$ fosse um corpo ordenado. Como consequência dessa suposição teríamos, em particular, $i^2 = -1 > 0$ e $1 > 0$. Da primeira dessas desigualdades segue que $1 < 0$ e da segunda que $0 < 1$. Daí, $1 < 1$ e, portanto, $1 \neq 1$, o que é impossível. Portanto, não há como transformar o corpo $\mathbb{C}$ num corpo ordenado.

**Proposição 39:** Sejam $a$, $b$ elementos arbitrários de um corpo ordenado $K$. Indicando-se o zero e a unidade desse corpo respectivamente por 0 e 1, tem-se:

(i) Se $a > 0$, então $a^{-1} > 0$, e se $a < 0$, então $a^{-1} < 0$.

(ii) Se $0 < a < 1$, então $1 < a^{-1}$, e se $1 < a$, então $0 < a^{-1} < 1$.

(iii) Se $b > a > 0$, então $b^{-1} < a^{-1}$.

(iv) Se $a < b < 0$, então $b^{-1} < a^{-1} < 0$.

*Demonstração:*

(i) Como $a > 0$, então $a \neq 0$ e, portanto, $a^{-1} \neq 0$, pois $aa^{-1} = 1$. Logo, $(a^{-1})^2 > 0$. Multiplicando-se ambos os membros da desigualdade $a > 0$ (hipótese) por $(a^{-1})^2$, obtém-se:

$$(a^{-1})^2 a > (a^{-1})^2 \cdot 0$$

desigualdade equivalente a $a^{-1} > 0$.

Deixamos a demonstração da segunda parte como exercício.

(ii) Como $a > 0$, então $a^{-1} > 0$, pelo que acabamos de demonstrar. Assim, multiplicando-se cada termo de $0 < a < 1$ por $a^{-1}$:

$$0 < 1 < a^{-1}$$

Deixamos a demonstração da segunda parte como exercício.

(iii) Sendo $a > 0$ e $b > 0$, então $a^{-1} > 0$ e $b^{-1} > 0$ e, portanto, $a^{-1}b^{-1} > 0$. Multiplicando-se cada termo de $b > a > 0$ por $a^{-1}b^{-1}$, obtém-se $a^{-1} > b^{-1} > 0$.

(iv) Como $a < 0$ e $b < 0$, então $a^{-1} < 0$ e $b^{-1} < 0$ e, portanto, $a^{-1}b^{-1} > 0$. Multiplicando-se cada termo de $a < b < 0$ por $a^{-1}b^{-1}$, obtém-se $b^{-1} < a^{-1} < 0$. #

**Proposição 40:** Sejam $a$ e $b$ elementos de um corpo ordenado $K$. Se $a < b$, então o corpo $K$ possui um elemento $c$ tal que $a < c < b$.

*Demonstração.* Como $a < b$, então $a + a < a + b$ ou $a \cdot 1_K + a \cdot 1_K < a + b$, ou, ainda, $a(2 \cdot 1_K) < a + b$. Analogamente, depois de se somar $b$ a cada um dos termos de $a < b$, obtém-se $a + b < b(2 \cdot 1_K)$. Portanto:

$$a(2 \cdot 1_K) < a + b < b(2 \cdot 1_K)$$

Mas, como já vimos (proposição 36), $2 \cdot 1_K > 0_K$ e, portanto, $(2 \cdot 1_K)^{-1} > 0_K$. Multiplicando-se cada termo de $a(2 \cdot 1_K) < a + b < b(2 \cdot 1_K)$ por $(2 \cdot 1_K)^{-1}$, o que não altera o sentido das desigualdades, pois $(2 \cdot 1_K)^{-1} > 0$, obtém-se:

$$a < (a + b)(2 \cdot 1_K)^{-1} < b$$

Então o elemento $c = (a + b)(2 \cdot 1_K)^{-1}$, que nos corpos $\mathbb{Q}$ e $\mathbb{R}$ é a média aritmética de $a$ e $b$, pertence a $K$ e está entre $a$ e $b$ (estritamente). #

**Corolário:** Nenhum corpo ordenado é um anel bem ordenado.

*Demonstração:* Seja $K$ um corpo ordenado e consideremos o seguinte subconjunto de $K$: $L = \{x \in K \mid x > 0_K\}$. Se $P$ indica o conjunto dos elementos positivos de $K$, então obviamente $L \subset P$. Mas, qualquer que seja $a \in L$ (por exemplo $a = 1_K$), a proposição nos assegura que $0_K < a(2 \cdot 1_K)^{-1} < a$, e, portanto, $L$ não tem mínimo. De onde $K$ não é bem ordenado, como queríamos provar. #

## Exercícios

**139.** Sejam $a, b, c, d$ elementos de um anel ordenado $A$. Prove que:

a) $b > 0$ se, e somente se, $a > a - b$.
b) Se $ab > 0$ e $b > 0$, então $a > 0$.
c) $a + b \geqslant a$ se, e somente se, $b \geqslant 0$.
d) $a + b > a$ se, e somente se, $b > 0$.
e) Se $a > b$ e $c < 0$, então $ac < bc$
f) Se $ab > 0$ e $b < 0$, então $a < 0$.
g) Se $a > b > 0$ e $c > d > 0$, então $ac > bd > 0$
h) Se $a > b$ e $c > d$, então $ac + bd > ad + bc$
i) $a^2 + b^2 \geqslant 2ab$.
j) Se $a \neq 0$ ou $b \neq 0$, então $a^2 + ab + b^2 > 0$

**Resolução**

a) $(\Rightarrow)$ Como $b > 0$, então $-b < 0$ ou $0 > -b$. Somando-se $a$ a cada um dos membros desta última desigualdade: $a > a - b$

h) Como $a > b$ e $c > d$, então $a - b > 0$ e $c - d > 0$. Assim, $(a - b)(c - d) > 0$ e, portanto, $ac - ad - bc + bd > 0$. De onde, $ac + bd > ad + bc$.

j) Se $a = 0$ e $b \neq 0$, então $a^2 + ab + b^2 = b^2 > 0$, pois $b \neq 0$. O raciocínio é análogo nos casos em que $a \neq 0$ e $b = 0$. Se $a > 0$ e $b > 0$, então $a^2 > 0$, $b^2 > 0$ e $ab > 0$. Portanto, $a^2 + b^2 + ab > 0$. Quando $a < 0$ e $b < 0$, a demonstração é análoga. Suponhamos agora que $a$ e $b$ tenham "sinais" diferentes. Então $ab < 0$ e, portanto, $-(ab) > 0$. Como, porém, $a^2 + b^2 + ab = (a + b)^2 + [-(ab)]$, em que $(a + b)^2 \geqslant 0$ e $[-(ab)] > 0$, então $a^2 + b^2 + ab > 0$. ■

**140.** Prove, por indução, que:

a) Se $a > 0$, então $a^n > 0$ $(n \in \mathbb{N})$.

b) Se $a < 0$, então $a^{2n} > 0$ $(n \in \mathbb{N})$.

c) Se $a < 0$, então $a^{2n+1} < 0$ $(n \in \mathbb{N})$.

d) Se $b > a > 0$, então $b^n > a^n$ $(n > 0)$.

**Resolução**

c) Se $n = 0$, então $a^{2n+1} = a < 0$ e, portanto a propriedade vale para $n = 0$. Seja $r$ um número natural e suponhamos que $a^{2r+1} < 0$. Então $a^{2(r+1)+1} = a^{2r+1} \cdot a^2 < 0$, uma vez que $a^{2r+1} < 0$, pela hipótese de indução, e $a^2 > 0$ pois $a \neq 0$. ■

**141.** Sejam $a, b$ elementos de um anel ordenado. Prove que:

a) $b > a$ se, e somente se, $b^3 > a^3$.

b) $a^3 = b^3$ se, e somente se, $a = b$.

c) As propriedades a) e b) valem também para $a^5$ e $b^5$? Prove ou contra-exemplifique.

**142.** Seja $K$ um corpo ordenado. Se $a$ é um elemento positivo de $K$, demonstre que, qualquer que seja o inteiro $n \geqslant 0$, $(a + 1_K)^n \geqslant n \cdot a + 1_K$.

**Resolução**

Como $(a + 1_K)^0 = 1_K$ e $0 \cdot a + 1_K = 1_K$, a propriedade vale para $n = 0$. Seja $r \geqslant 0$ um inteiro e suponhamos que $(a + 1_K)^r \geqslant r \cdot a + 1_K$. Considerando-se que $a$ é positivo e que, desse modo, $a + 1_K > 0$, então $(a + 1_K)^r(1_K + a) \geqslant (r \cdot a + 1_K)(1_K + a)$, ou seja, $(a + 1_K)^{r+1} \geqslant (r \cdot a + 1_K)(1 + a) = r \cdot a + (r \cdot a)a + 1_K + a = (r + 1) \cdot a + (r \cdot a)a + 1_K$. Mas, como $a \geqslant 0$, então $r \cdot a \geqslant 0$ e, assim, $(r \cdot a)a \geqslant 0$. Somando-se $(r + 1) \cdot a + 1_K$ a ambos os membros da última desigualdade, obtém-se $(r + 1) \cdot a + 1_K + (r \cdot a)a \geqslant (r + 1) \cdot a + 1_K$. Portanto, $(a + 1_K)^{r+1} \geqslant (r + 1) \cdot a + 1_K$. ■

**143.** Seja $A$ um anel ordenado. Demonstre que $A$ é arquimediano se, e somente se, para qualquer $a \geq 1_K$ e qualquer $b$, existe $n \in \mathbb{N}$ tal que $n \cdot a > b$.

**144.** Sejam $a, b$ elementos de um corpo arquimediano $K$. Demonstre que:

a) Se $a > 1_K$, então existe $n \in \mathbb{N}$ tal que $a^n > b$

b) Se $a > 1_K$ e $b$ é positivo, então existe $n \in \mathbb{N}$ tal que $a^{-n} < b$

**Resolução**

a) Como $a > 1_K$, então $a - 1_K$ é positivo. Logo, devido ao exercício 142 anterior, $(a - 1_K + 1_K)^m \geq m \cdot (a - 1_K) + 1_K$ ou $a^m \geq m \cdot a - m \cdot 1_K + 1_K$, para qualquer $m \geq 0$. Mas, como $K$ é arquimediano, existe $n \in \mathbb{N}$ tal que $n \cdot a > b + n \cdot 1_K - 1_K$ ou $n \cdot a - n \cdot 1_K + 1_K > b$.

Portanto, $a^n > b$. ∎

**145.** Seja $A$ um anel bem ordenado. Prove que, qualquer que seja o inteiro $n$, o conjunto $\{a \in A \mid n \cdot 1_A < a < (n + 1) \cdot 1_A\}$ é vazio.

**146.** Seja $A$ um anel bem ordenado. Demonstre que $A = \mathbb{Z} \cdot 1_A$.

**Resolução**

Seja $a \in A$. Como um anel bem ordenado é arquimediano, então, para algum inteiro $n > 0$, tem-se $n \cdot 1_A > a$. Sendo $r$ o menor número natural estritamente positivo tal que $r \cdot 1_A > a$: $(r - 1) \cdot 1_A \leq a < r \cdot 1_A$.

Assim, como decorrência do exercício anterior, $(r - 1) \cdot 1_A = a$ e, portanto, $a \in \mathbb{Z} \cdot 1_A$. ∎

**147.** Seja $A$ um anel. Se $L$ é um subconjunto não vazio de $A$, definem-se $L + L$, $L \cdot L$ e $-L$ da seguinte maneira:

$$L + L = \{x + y \mid x, y \in L\}, L \cdot L = \{xy \mid x, y \in L\}, -L = \{-x \mid x \in L\}$$

Isso posto, seja $A$ um anel de integridade. Demonstre que uma condição necessária e suficiente para que se possa definir uma relação de ordem sobre $A$, compatível com as operações desse anel, é que exista um subconjunto não vazio $P \subset A$ tal que: (i) $P + P \subset P$; (ii) $P \cdot P \subset P$; (iii) $P \cup (-P) = A$; (iv) $P \cap (-P) = \{0_A\}$.

*Sugestão:* Se $A$ é um anel ordenado, mostre que o conjunto $P$ dos elementos positivos do anel cumpre as condições do enunciado. Para demonstrar a recíproca, defina $\leq$ assim: $x \leq y$ se $y - x \in P$. Observe que os elementos positivos do anel serão exatamente os elementos de $P$.

**148.** a) Sejam $A$ um anel ordenado e $K$ seu corpo de frações. Mostre que o conjunto

$$P = \left\{ \frac{a}{b} \in K \mid ab \geq 0 \right\}$$

cumpre as condições (i), (ii), (iii), (iv) do exercício anterior e que, portanto, a relação $\leqslant$ sobre $K$ definida por $\frac{a}{b} \leqslant \frac{c}{d}$ se, e somente se, $\left(\frac{c}{d} \quad \frac{a}{b}\right) \in P$ faz de $K$ um corpo ordenado.

b) Mostre que $\frac{a}{b} \leqslant \frac{c}{d}$ se, e somente se, $acb^2 \geqslant abd^2$.

c) Se $a, b \in A$, prove que $a \leqslant b$ (em $A$) se, e somente se, $\frac{a}{1} \leqslant \frac{b}{1}$ (em $K$). (Por isso se diz que a ordem definida em $K$ é uma "extensão" da ordem do anel $A$.)

*Sugestão:* Como uma fração pode ser representada de mais de uma maneira, é preciso mostrar primeiro que, se $r \in K$ e $r = \frac{a}{b} = \frac{c}{d}$, então $\frac{a}{b} \in P$ se, e somente se, $\frac{c}{d} \in P$. Ora, de $\frac{a}{b} = \frac{c}{d}$ segue que $ad = bc$ e, daí, multiplicando-se ambos os membros dessa igualdade por $ac$, que $a^2cd = abc^2$. Mas, como $a^2 \geqslant 0$ e $c^2 \geqslant 0$, então $cd \geqslant 0$ se, e somente se, $ab \geqslant 0$.

CAPÍTULO VI

# ANÉIS DE POLINÔMIOS

## 1. NOTA HISTÓRICA

Ao se iniciar o século XVI, o ponto alto das realizações matemáticas ainda eram as obras clássicas gregas. Destas, certamente a mais conhecida e estudada eram os *Elementos*, de Euclides (c. século III a.C.), embora outras a superassem em originalidade.

Ocorre que, das três partes em que se poderia dividir a matemática da época, geometria, aritmética e álgebra, aquela em que os gregos do período clássico menos se destacaram foi a álgebra. Nesse campo, a linguagem algébrica, de que prescindiam, era substituída, com óbvias desvantagens, pela linguagem geométrica.

É verdade que posteriormente, no século II ou III de nossa era, um grego chamado Diofanto introduziu símbolos para indicar a variável e suas potências (até a de expoente 6), porém esse passo inicial não teve continuidade imediata.

Na primeira metade do século XVI, verificou-se um grande avanço no desenvolvimento da teoria das equações algébricas com a descoberta de fórmulas algébricas para a resolução de equações de grau 3 e 4. Mas o raciocínio dos matemáticos que conseguiram esses grandes feitos era ainda geométrico e a linguagem verbal.

Em 1591, o francês François Viète (1540-1603), em sua obra *Introdução à arte analítica* (*In arten analyticem isagoge*), criou o cálculo literal, ou seja, introduziu a linguagem das formulas na matemática. Pela primeira vez na história da matemática tornou-se possível escrever genericamente, por exemplo, uma equaçao do segundo

grau. No entanto, a notação usada por Viète, que consistia em representar por vogais e consoantes maiúsculas respectivamente as variáveis e as constantes, não vingou. Porém representar constantes por letras, algo que hoje nos parece corriqueiro, foi uma revolução na matemática.

O trabalho de Viète teve continuidade com o também francês René Descartes (1596-1650), um homem cuja preocupação intelectual maior era a filosofia, a serviço da qual colocou suas pesquisas matemáticas. Sua única obra matemática, *Geometria* (*Géomètrie*), tinha por objetivo usar o potencial da álgebra na resoluçao de problemas geométricos clássicos. Entendendo que a geometria clássica "não exercita o intelecto sem cansar muito a imaginação" e que a álgebra renascentista que herdara submetia as letras a regras tais que, "em vez de se transformar numa autêntica ciência, torna-se uma arte confusa que obscurece a mente", Descartes procurou estabelecer uma vinculação entre esses dois ramos da matemática que aproveitasse "o melhor da análise geométrica e da álgebra para corrigir os defeitos de uma pela outra". A publicação dessa obra representa o marco inicial da criação da geometria analítica.

Para embasar seu trabalho, Descartes teve de dar contribuições próprias para o desenvolvimento da álgebra. É o caso, por exemplo, do princípio de identidade de polinômios (de que falaremos neste capítulo), que possivelmente usou pela primeira vez na história da matemática. Diga-se de passagem, porém, que nas contribuições de Descartes à matemática não se nota nenhuma preocupação com enunciados e formalismos teóricos. Vale acrescentar ainda que tanto a moderna notação algébrica — o uso das letras $x$, $y$, $z$ para indicar variáveis e $a$, $b$, $c$, ... para indicar constantes ou parâmetros — como a notação exponencial para indicar potências foram introduzidas por Descartes na obra citada.

Conceitos algébricos mais sutis, como, por exemplo, o de polinômio irredutível, só seriam estudados cerca dois séculos e meio depois, na esteira das transformações profundas pelas quais a álgebra passou na primeira metade do século XIX.

## 2. CONSTRUÇÃO DO ANEL DE POLINÔMIOS

No que segue, em todo este capítulo, indicaremos por $A$ um anel de integridade infinito. Eventualmente esse anel pode ser um corpo infinito, caso em que será indicado por $K$. Os exemplos mais importantes de anéis de integridade infinitos obviamente são $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Uma funçao $f: A \to A$ denomina-se *função polinomial sobre A* se existem elementos $a_0, a_1, ..., a_r$ em $A$ tais que, para todo $x \in A$:

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$$

Quando se escreve $f(x)$ como acima, com os expoentes da variável em ordem crescente, a expressão do segundo membro será referida como uma *forma padrão* para a função polinomial.

Essa definição suscita desde logo a seguinte questão: pode uma função polinomial ter mais do que uma forma padrão? Ou seja, pode outra sequência, $b_0, b_1, b_2, ..., b_s$ de elementos de $A$, definir a mesma *função* polinomial $f$? Isso significaria a possibilidade de

$$f(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s$$

para todo $x \in A$. Mostraremos que no presente caso ($A$ anel de integridade infinito) isso não é possível. Já levando em conta esse fato, poderemos nos permitir usar, desde logo, a expressão *polinômio sobre* A com o mesmo sentido de "função polinomial sobre $A$". De fato, a idéia de polinômio como uma expressão formal do tipo

$$a_0 + a_1x + a_2x^2 + ... + a_rx^r$$

em que $x$ é um símbolo que pode representar um elemento do anel ou não, pressupõe a unicidade da seqüência $a_0, a_1, ..., a_r$.

A *adição* de dois polinômios quaisquer, $f$ e $g$, dados respectivamente por $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ e $g(x) = b_0 + b_1x + b_2x^2 + ... + b_tx^t$, naturalmente se enquadra no conceito de adição de funções cujo contradomínio é um anel: a *soma* $f + g$ é definida por $(f + g)(x) = f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ...$ Convém observar que, ao escrever a expressão final, já levamos em conta as propriedades operatórias de um anel. A expressão obtida para $(f + g)(x)$ mostra que $f + g$ também é um polinômio sobre $A$. Isso posto, pode-se demonstrar que o par formado pelo conjunto dos polinômios sobre $A$ e a adição assim introduzida é um grupo abeliano. Aqui apenas destacaremos que o elemento neutro é a função identicamente nula de $A$ (que é uma função polinomial, chamada *polinômio identicamente nulo*, pois pode ser definida por $0 + 0 \cdot x + 0 \cdot x^2 + ...$, em que 0 indica o zero do anel $A$) e que o simétrico aditivo de um polinômio $f$, com forma padrão $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$, é o polinômio $-f$ definido por $(-f)(x) = -a_0 + (-a_1)x + (-a_2)x^2 + ... + (-a_r)x^r$.

Para introduzir a *multiplicação* de dois polinômios quaisquer, $f$ e $g$, obviamente vale também a observação anterior. Então, mantidas as notações do parágrafo anterior, o *produto* $fg$ é assim definido:

$$(fg)(x) = f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ... + (a_rb_s)x^{r+s}$$

Também aqui, para obter a expressão final utilizamos as propriedades algébricas de $A$. Percebe-se, pela expressão obtida, que $fg$ também é um polinômio sobre $A$. Por exemplo, se $f(x) = 1 + 2x - 2x^3$ e $g(x) = -x + 3x^2$, então $(fg)(x) = 1 \cdot 0 + [1 \cdot (-1) + 2 \cdot 0]x + [1 \cdot 3 + 2 \cdot (-1) + 0 \cdot 0]x^2 + [1 \cdot 0 + 2 \cdot 3 + 0 \cdot (-1) + (-2) \cdot 0]x^3 + [1 \cdot 0 + 2 \cdot 0 + 0 \cdot 3 + (-2)(-1) + 0 \cdot 0]x^4 + [(-2) \cdot 3]x^5 = -x + x^2 + 6x^3 + 2x^4 - 6x^5$.

Pode-se demonstrar (aqui apenas mencionaremos) que para a multiplicação de polinômios valem a *associatividade* e a *comutatividade* e que o polinômio definido por $1 + 0 \cdot x + 0 \cdot x^2 + ...$, em que 0 e 1 indicam respectivamente o zero e a

unidade de $A$, é o *elemento neutro* dessa operação. Como, ademais, pode-se provar também que a multiplicação é distributiva em relação à adição, concluímos que o conjunto das funções polinomiais sobre um anel de integridade $A$, com a adição e a multiplicação definidas acima, é um anel comutativo com unidade. Esse anel será indicado por $A[x]$, o que pressupõe naturalmente a variável indicada por $x$.

Mas $A[x]$ não é um corpo, como mostraremos. De fato, tomemos, por exemplo, o polinômio $f(x) = x$. Obviamente $f(x)$ não é o polinômio identicamente nulo. Se $f(x)$ fosse inversível, existiria um polinômio $g(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$, com $a_r \neq 0$, tal que $f(x) \cdot g(x) = a_0x + a_1x^2 + ... + a_rx^{r+1} = 1$ (unidade do anel), para todo $x \in A$. Assim, para $x = 0$ (zero do anel), teríamos o seguinte absurdo: $0 = 1$. Exibindo um polinômio não nulo de $A[x]$ que não é inversível, fica provado que esse anel não é um corpo.

Se $a \in A$, o polinômio $f$ definido por $f(x) = a$, para qualquer $x \in A$, é chamado *polinômio constante* determinado por $a$. Se $a \neq 0$ é um elemento inversível de $A$, o polinômio constante correspondente $f$ é necessariamente inversível: seu inverso é o polinômio constante $g$ definido por $a^{-1}$ pois, para todo $x \in A$ vale $(fg)(x) = f(x)g(x) = aa^{-1} = 1$ (unidade de $A$). Obviamente no caso de $A$ ser um corpo, todos os polinômios constantes, exceto o polinômio nulo, são inversíveis. Surge então a pergunta: há outros polinômios inversíveis, além desses? Veremos, ao final da próxima seção, que não.

## Exercícios

Nos exercícios deste capítulo, quando não se explicitar o universo dos coeficientes de polinômios ou equações envolvidas, fica subentendido que se trata de $\mathbb{C}$ (corpo dos complexos).

**1.** Seja a função polinomial sobre $\mathbb{Z}$, dada por $f(x) = x^{15} + x^{14} + x^{13} + ... + x^2 + x + 1$. Calcule $f(0)$, $f(1)$ e $f(-1)$.

**2.** Seja $p(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ um polinômio e observe $p(1) = a_n + a_{n-1} + ... + a_1 + a_0$, soma dos coeficientes do polinômio $p(x)$. Qual a soma dos coeficientes do polinômio $(4x^3 - 2x^2 - 2x - 1)^{36} \in \mathbb{R}[x]$?

**3.** Dados os polinômios sobre $\mathbb{Z}$:
$f(x) = 7 - 2x + 4x^2$, $g(x) = 5 + x + x^2 + 5x^3$, $h(x) = 2 - 3x + x^4$
calcule $(f + g)(x)$, $(g - h)(x)$ e $(h - f)(x)$.

**4.** Dados os polinômios sobre $\mathbb{Z}$.
$f(x) = 2 + 3x - 4x^2$, $g(x) = 7 + x^2$, $h(x) = 2x - 3x^2 + x^3$
calcule $(fg)(x)$, $(gh)(x)$ e $(hf)(x)$.

**5.** Supondo o polinômio sobre $\mathbb{R}$ dado por $f(x) = (c - a - 1) + (b - c + 5)x + (a - b - 2)x^2 + (a - 1)x^3$ inversível, determine $a$, $b$, $c$ e $f^{-1}$.

**6.** Prove que, se $B$ é um subanel de $A$, então $B[x]$ é um subanel de $A[x]$

**7.** Verifique se cada conjunto abaixo é um subanel de $\mathbb{Z}[x]$.

$A = \{a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x] \mid a_0 \in 2\mathbb{Z}\}$
$B = \{a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x] \mid a_0 = 0\}$
$C = \{a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x] \mid a_0 + a_1 = 0\}$

Algum deles é ideal em $\mathbb{Z}[x]$?

## 3. POLINÔMIOS IDÊNTICOS

**3.1** Na seqüência, precisaremos do fato de que, se $u \in A$, vale a seguinte identidade em $A[x]$:

$$x^n - u^n = (x - u)(x^{n-1} + ux^{n-2} + ... + u^{n-2}x + u^{n-1}) \qquad (1)$$

para qualquer inteiro $n > 0$ e todo $x \in A$. A verificação desse fato pode ser feita informalmente, efetuando-se a multiplicação indicada no segundo membro e simplificando-se o resultado:

$$x^n + ux^{n-1} + ... + u^{n-2}x^2 + u^{n-1}x - (ux^{n-1} + u^2x^{n-2} + ... + u^{n-1}x + u^n) = x^n - u^n$$

Seja $f$ um polinômio não constante. Então $f$ tem uma forma padrão do tipo $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$, com $a_r \neq 0$, para algum $r > 0$. Logo, para qualquer $u \in A$, tem-se:

$$f(x) - f(u) = a_1(x - u) + a_2(x^2 - u^2) + ... + a_r(x^r - u^r)$$

Usando-se (1) em cada parcela do segundo membro e a distributividade da multiplicação em relação à adição, para pôr $(x - u)$ em evidência, obtém-se:

$f(x) - f(u) =$
$(x - u)[a_1 + a_2(x + u) + a_3(x^2 + ux + u^2) + ... + a_r(x^{r-1} + ux^{r-2} + ... + u^{r-1})] =$
$(x - u)[(a_1 + a_2u + ... + a_ru^{r-1}) + (a_2 + a_3u + ... + a_ru^{r-2})x + ... + a_rx^{r-1}] = (x - u)q(x)$
e daí:

$$f(x) = (x - u)q(x) + f(u)$$

em que o fator $q(x)$ que multiplica $x - u$ também define um polinômio de $A[x]$. É importante observar que $q(x)$ tem forma padrão do tipo:

$$f(x) = ... + a_rx^{r-1}$$

em que, por hipótese, $a_r \neq 0$.

**Definição 1:** Seja $f$ um polinômio sobre $A$. Um elemento $u \in A$ é chamado *raiz* de $f$ se $f(u) = 0$ (zero do anel)

*Exemplo 1:* Consideremos o polinômio $f \in \mathbb{C}[x]$ assim definido. $f(x) = x^2 + 1$. Os números complexos $i$ e $-i$ são raízes de $f$, pois $f(i) = f(-i) = 0$.

*Exemplo 2:* Seja $a$ um elemento não nulo de um anel de integridade infinito $A$. Então o polinômio constante $f$ definido por $a$, ou seja, o polinômio que admite a forma padrão $f(x) = a$, não tem nenhuma raiz, pois, para todo $u \in A$, $f(u) = a \neq 0$.

*Exemplo 3:* Todos os elementos de um anel de integridade infinito $A$ são raízes do polinômio identicamente nulo sobre esse anel. De fato, a imagem de todo elemento de $A$ por esse polinômio é, por definição, o zero do anel. Logo, o polinômio identicamente nulo tem infinitas raízes — todos os elementos de $A$.

**Proposição 1:** Seja $u$ uma raiz de um polinômio não constante $f \in A[x]$. Se $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$, com $a_r \neq 0$, para todo $x \in A$, então $f(x) = (x - u)q(x)$, para algum polinômio $q$ com uma forma padrão do seguinte tipo: $q(x) = ... + a_rx^{r-1}$.

*Demonstração:* Como já vimos, $f(x) = (x - u)q(x) + f(u)$, para algum $q \in A[x]$, com forma padrão do tipo $q(x) = ... + a_rx^{r-1}$, com $a_r \neq 0$, qualquer que seja $x \in A$. Mas, como $u$ é raiz de $f$, então $f(u) = 0$ (zero de $A$) e, portanto, $f(x) = (x - u)q(x)$, como queríamos mostrar. #

**Corolário:** Seja $f \in A[x]$ assim definido: $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$, com $a_r \neq 0$. Se $u_1, u_2, ..., u_m$ são raízes de $f$, então:

$$f(x) = (x - u_1)(x - u_2)...(x - u_m)q_m(x)$$

em que $q_m$ é um polinômio de $A[x]$ que admite uma forma padrão do tipo $q_m(x) = ... + a_rx^{r-m}$, para todo $x \in A$. Ademais, qualquer outra eventual raiz de $f$ é raiz de $q_m$.

*Demonstração:* A rigor, deveríamos proceder por indução, mas pouparemos o estudante do formalismo desse método. Como $u_1$ é raiz de $f$, a proposição 1 garante que $f(x) = (x - u_1)q_1(x)$, para algum $q_1 \in A[x]$, que admite forma padrão do tipo $q_1(x) = ... + a_rx^{r-1}$, qualquer que seja $x \in A$. Mas, como $u_2$ também é raiz de $f$, então $f(u_2) = (u_2 - u_1)q_1(u_2) = 0$. Considerando que $u_2 - u_1 \neq 0$ e que estamos num anel de integridade, então $q_1(u_2) = 0$ e, portanto, $u_2$ é raiz de $q_1$. Sendo assim, podemos concluir, ainda com base na proposição 1, que $q_1(x) = (x - u_2)q_2(x)$, para algum $q_2 \in A[x]$, que admite forma padrão do tipo $q_2(x) = ... + a_rx^{r-2}$, para todo $x \in A$. De onde:

$$f(x) = (x - u_1)(x - u_2)q_2(x)$$

Esse raciocínio, usado ainda com $u_3, u_4, ..., u_m$, levará à conclusão proposta, ou seja, que

$$f(x) = (x - u_1)(x - u_2)...(x - u_m)q_m(x)$$

para algum $q_m \in A[x]$, que admite forma padrão do tipo $q_m(x) = ... + a_rx^{r-m}$, para todo $x \in A$

Agora, se $v \in A$ também é uma raiz de $f$, diferente das raízes consideradas, então:

$$f(v) = (v - u_1)(v - u_2) \dots (v - u_r)q_m(v) = 0$$

O fato de $(v - u_1)(v - u_2) \dots (v - u_r) \neq 0$ implica então, dado que $A$ é anel de integridade, que $q_m(v) = 0$. Ou seja, $v$ é raiz de $q_m$. #

**Proposição 2:** Seja $f \in A[x]$ um polinômio assim definido. $f(x) = a_0 + a_1x + + a_2x^2 + \dots + a_rx^r$, com $a_r \neq 0$ (zero de $A$). Então $f$ tem $r$ raízes, no máximo, em $A$

*Demonstração:* No caso em que $f$ não tem nenhuma raiz em $A$, a proposição é verdadeira, pois $r \geq 0$. Mas, se $u_1, \dots, u_m \in A$ são raízes de $f$, então, devido ao corolário da proposição 1, $f(x) = (x - u_1)\dots(x - u_m)q(x)$, para algum $q \in A[x]$, que admite uma forma padrão do seguinte tipo: $q(x) = \dots + a_rx^{r-m}$, para todo $x \in A$. Ademais, qualquer outra raiz de $f$ (se existisse) teria de ser raiz de $q$. Mas, se $m = r$, $q$ será definido por $q(x) = a_r$ e, portanto, não tem nenhuma raiz em $A$, pois $a_r \neq 0$ (exemplo 2). Isso mostra que o número de raízes de $f$ não pode ultrapassar $r$, como queríamos provar. #

*Exemplo 4:* Se $A = \mathbb{Z}$ (inteiros), $A = \mathbb{Q}$ (racionais) ou $A = \mathbb{R}$ (reais), então um polinômio sobre $A$ pode ter um número de raízes menor que seu grau. Por exemplo, o polinômio $f$ definido por $f(x) = x^2 + 1$ não tem nenhuma raiz em $\mathbb{R}$ e, portanto, nenhuma em $\mathbb{Q}$ nem em $\mathbb{Z}$. Quanto a isso, o comportamento do corpo $\mathbb{C}$ é diferente, como veremos posteriormente.

A esta altura temos condições de responder a uma questão importante: é possível representar o polinômio identicamente nulo (que tem infinitas raízes — todos os elementos do anel $A$) por uma expressão polinomial, na forma padrão, em que nem todos os parâmetros sejam iguais a zero? A resposta é não, porque essa expressão poderia ser escrita como

$$a_0 + a_1x + \dots + a_rx^r$$

com $a_r \neq 0$ (zero do anel), e, portanto, teria no máximo $r$ raízes (lembrar que, como foi visto no exemplo 3, o polinômio identicamente nulo tem infinitas raízes).

**Proposição 3** (princípio de identidade de polinômios): Sejam $f$ e $g$ polinômios de $A[x]$, que admitem forma padrão do tipo $f(x) = a_0 + a_1x + \dots + a_rx^r$ e $g(x) = b_0 + + b_1x + \dots + b_sx^s$, para todo $x \in A$. Então $f = g$ se, e somente se, $a_1 = b_1, a_2 = b_2, \dots$

*Demonstração:* É imediato que, se $a_1 = b_1, a_2 = b_2, \dots$, então $f = g$. Para demonstrar a recíproca, observemos primeiro que o polinômio $f - g$ é definido assim:

$$(f - g)(x) = f(x) - g(x) = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \dots$$

para todo $x \in A$. Mas, devido à hipótese de que $f$ e $g$ são iguais, então, para todo $u \in A$ vale a igualdade $f(u) = g(u)$ e, portanto, $(f - g)(u) = f(u) - g(u) = 0$ (zero de $A$). Ou seja, todo elemento de $A$ é raiz de $f - g$, que, portanto, tem infinitas raízes. Logo, considerando-se a proposição anterior e o exemplo 3, $f - g$ é o polinômio

identicamente nulo sobre $A$. Então $a_1 - b_1 = a_2 - b_2 = \dots = 0$ e, portanto, $a_1 = b_1$, $a_2 = b_2$, ..., como queríamos demonstrar. #

A proposição 3 garante que num polinômio $f$, dado na forma padrão por $f(x) = a_0 + a_1x + \dots + a_rx^r$, a seqüência $a_0, a_1, \dots, a_r$ está univocamente determinada. Os elementos dessa seqüência são chamados *coeficientes* de $f$. Em particular, se $f$ não é o polinômio identicamente nulo, então, para algum índice $m$, com $0 \leq m \leq r$, tem-se $a_m \neq 0$ (zero do anel) e $a_{m+1} = \dots = a_r = 0$ (zero do anel). Neste caso, $a_m$ é chamado *coeficiente dominante* de $f$.

## 3.2 Grau

Agora estamos em condições de definir o *grau de um polinômio não nulo*: é simplesmente o índice de seu coeficiente dominante. Adotada a notação $\partial$ para indicar o grau, então, por exemplo, $\partial(1 + x^2) = 2$ e $\partial(5) = 0$. Com isso, a proposição 2 pode ser formulada em termos do grau da seguinte maneira: "Se o grau de um polinômio $f$ sobre o anel de integridade infinito $A$ é $r$, então o número de raízes de $f$ em $A$ é menor que ou igual a $r$".

É importante destacar, ainda, a seguinte propriedade: Se $f$ e $g$ são polinômios não nulos, então $\partial(f \cdot g) = \partial(f) + \partial(g)$. De fato, se os coeficiente dominantes de $f$ e $g$ são, respectivamente, $a_r$ e $b_s$, então $f(x) = \dots + a_rx^r$ e $g(x) = \dots + b_sx^s$ e, portanto, a forma padrão de $fg$ é do tipo

$$(fg)(x) = \dots + a_rb_sx^{r+s}$$

Como $a_rb_s \neq 0$, já que os fatores são elementos não nulos do anel de integridade $A$, então $\partial(fg) = r + s = \partial(f) + \partial(g)$.

Nesta altura temos condições de mostrar que $A[x]$ também é um anel de integridade. De fato, dados dois polinômios não identicamente nulos, $f$ e $g$, de coeficientes dominantes $a_r$ e $b_s$, então o produto desses polinômios é dado, na forma padrão, por

$$(fg)(x) = \dots + a_rb_sx^{r+s}$$

Como $a_rb_s \neq 0$, pois $a_r$ e $b_s$ são elementos não nulos do anel de integridade $A$, então $fg$ também não é identicamente nulo.

*Exemplo 5:* Se $f$ e $g$ são polinômios sobre $A$ de graus $r$ e $s$, respectivamente, e se $f + g$ não é identicamente nulo, então $\partial(f + g) \leq max\{\partial(f), \partial(g)\}$. Suponhamos que as formas padrões de $f$ e $g$ sejam, respectivamente, $f(x) = \dots + a_rx^r$ $(a_r \neq 0)$ e $g(x) = \dots + b_sx^s$ $(b_s \neq 0)$. Se $r = s$, então $(f + g)(x) = \dots + (a_r + b_r)x^r$, o que mostra que $\partial(f + g) \leq \partial(f) = max\{\partial(f), \partial(g)\}$. (Notar que o caso $\partial(f + g) < \partial(f)$ ocorre quando $a_r + b_r = 0$.) Se $r > s$, então:

$$(f + g)(x) = \dots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \dots + a_rx^r$$

Isso mostra que $\partial(f + g) = \partial(f) = max\{\partial(f), \partial(g)\}$. Analogamente se procede no caso em que $s > r$.

### 3.3 Imersão de $A$ em $A[x]$

Para encerrar esta seção, mostraremos que $A$ é um subanel unitário de $A[x]$ e em que termos se dá essa inclusão. A idéia é identificar cada polinômio constante com o elemento do anel $A$ que o determina. Formalmente isso corresponde a introduzir a aplicação

$$\sigma: A \to A[x]$$

que associa a cada $a \in A$ o polinômio constante $f_a$, dado por $f_a(x) = a$, para todo $x$ de $A$, e mostrar que $\sigma$ é um homormofismo injetor de anéis. De fato.

- $\sigma(a + b) = f_{a+b}$, em que $f_{a+b}(x) = a + b$, para todo $x$ de $A$. Como, porém, $(f_a + f_b)(x) = f_a(x) + f_b(x) = a + b$, então $f_{a+b}(x) = (f_a + f_b)(x)$, para todo $x$ de $A$ e, portanto, $f_a + f_b = f_{a+b}$. Logo:

$$\sigma(a + b) = f_{a+b} = f_a + f_b = \sigma(a) + \sigma(b)$$

- Analogamente se demonstra que:

$$\sigma(ab) = \sigma(a)\sigma(b)$$

- $\sigma$ é injetora, pois, se $a \neq b$, então $f_a \neq f_b$, já que, por exemplo, $f_a(1_A) = a$ e $f_b(1_A) = b$. Portanto, $\sigma(a) \neq \sigma(b)$.

Então $A$ é isomorfo à sua imagem $\sigma(A)$ em $A[x]$ e, portanto, pode ser considerado um subanel de $A[x]$. É por esse ângulo que devemos interpretar a inclusão $A \subset A[x]$. #

Podemos mostrar agora que o conjunto dos polinômios inversíveis coincide com o conjunto dos elementos inversíveis do anel $A$. De fato, se $f \in A[x]$ é inversível, então $fg = 1$, para um conveniente polinômio $g$ sobre $A$. Daí: $\partial(f) + \partial(g) = \partial(1) = 0$. Logo, $\partial(f) = \partial(g) = 0$ e, portanto, $f$ e $g$ são polinômios constantes inversíveis, o que significa, considerando-se a identificação proporcionada pela proposição anterior, que são elementos de $A$. Por outro lado, como já vimos, se $c \in A$ é inversível, então o polinômio $f$ determinado por $c$, isto é, o polinômio definido por $f(x) = c$, é inversível e seu inverso é o polinômio $g$ definido por $g(x) = c^{-1}$.

#### Exercícios

**8.** Determine o polinômio $P(x)$ de grau 3 cujas raízes são 1, 2 e 3, sabendo que $P\left(\frac{1}{2}\right) = -\frac{15}{8}$.

**9.** Seja $f$ uma função real tal que $f(x) = ax^3 + bx^2 + cx + d$ para todo $x \in \mathbb{R}$, em que $a$, $b$, $c$ e $d$ são números reais. Se $f(x) = 0$, para todo $x$ do conjunto $\{1, 2, 3, 4, 5\}$, calcule $f(6)$.

**10.** Determine $a$, $b$ e $c$ de modo que a função $f(x) = (a + b - 5)x^2 + (b + c - 7)x + (a + c)$ seja identicamente nula.

**11.** Dadas as funções polinomiais $f(x) = (a - 1)x^2 + bx + c$ e $g(x) = 2ax^2 + 2bx - c$, qual é a condição para que se tenha $f = g$?

**12.** Qual o valor de $a - b$ para que o binômio $2x^2 + 17$ seja idêntico à expressão $(x^2 + b)^2 - (x^2 - a^2)(x^2 + a^2)$, com $a > 0$ e $b > 0$?

**13.** Dados os polinômios $f = x^2$, $g = x^2 + x^4$, $h = x^2 + x^4 + x^6$ e $k = 3x^6 - 6x^4 + 2x^2$, obtenha os números reais $a, b, c$ de modo que se tenha $k = af + bg + ch$.

**14.** Seja $f \in K(x)$, $f \neq 0$ e $\partial f = 3$, em que $K$ é um corpo; se $a$, $b$ e $c$ são três elementos distintos de $K$, mostre que se podem determinar, de modo único, elementos $p$, $q$, $r$ e $s$ em $K$, tais que $f = p + q(x - a) + r(x - a)(x - b) + s(x - a)(x - b)(x - c)$.

**15.** Discuta, em função de $a$, o grau do polinômio $f(x) = (2a^2 + a - 3)x^3 + (a^2 - 1)x^2 + (a + 1)x - 3$.

**16.** Sejam $A$ um anel de integridade e $f, g \in A[x]$ tais que $\partial(f + g) = 5$ e $\partial(f - g) = 2$. Determine $\partial(fg)$, $\partial(f^2 - g^2)$ e $\partial(f^2 + g^2)$.

**17.** Sendo $A$ um anel de integridade infinito e sabendo que $f, g \in A[x]$ são tais que $\partial f^2 = 8$, $\partial(fg) = 7$, determine $\partial(f - g)$, $\partial f^3$, $\partial g^2$ e $\partial(f + g)^3$.

**18.** Determine a condição para que um polinômio real $ax^2 + bx + c$ seja um quadrado perfeito.

**Resolução**

$ax^2 + bx + c$ é um polinômio quadrado perfeito se existir $px + q$ tal que $ax^2 + bx + c = (px + q)^2$; então: $ax^2 + bx + c = p^2x^2 + 2pqx + q^2$.

Aplicando a proposição 3, temos:

(I) $a = p^2$; (II) $b = 2pq$; (III) $c = q^2$.

Quadrando (II), temos $b^2 = 4p^2q^2$ (II').

Substituindo (I) e (III) em (II'), vem $b^2 = 4(p^2)(q^2) = 4ac$.

Resposta: $b^2 = 4ac$.

Essa condição também é suficiente. ■

**19.** Determine a condição para que o polinômio $f = (ax + b)^2 + (cx + d)^2$, em que $a$, $b$, $c$ e $d$ são reais e não nulos, seja um quadrado perfeito.

**20.** Determine $a \in K$ de modo que o polinômio $ax^2$ seja um quadrado perfeito em $K[x]$, nos seguintes casos:

a) $K = \mathbb{Q}$

b) $K = \mathbb{R}$

c) $K = \mathbb{C}$

**21.** Mostre que não existe um polinômio $f \in \mathbb{R}[x]$ tal que $f^2(x) = f(x)\,f(x) = 1 + x + x^3$.

**22.** O coeficiente da maior potência de um polinômio $P(x)$ do 3º grau é 1. Sabendo que $P(1) = P(2) = 0$ e $P(3) = 30$, calcule $P(-1)$.

**23.** a) Determine os polinômios $f$ do 3º grau tais que $f(x) - f(x-1) = x^2$, para todo $x \in \mathbb{R}$.

b) Usando o resultado do item *a*, calcule em função de $n$ a soma $S = 1^2 + 2^2 + 3^2 + \dots + n^2$.

**24.** Mostre que, se $K$ é um corpo infinito, então existem funções de $K$ em $K$ não polinomiais.

**Resolução**

Consideremos a aplicação $f: K \to K$ tal que $f(0) = 1$ e $f(x) = 0$, para todo $x \in K^*$. Como $f$ admite infinitas raízes em $K$ e $f$ não é nula, então $f$ não é polinomial. ■

**25.** Mostre que as funções trigonométricas seno e cosseno não são funções polinomiais.

*Sugestão.* Verifique que $\operatorname{sen} x = 0$ e $\cos x = 0$ têm infinitas raízes.

## 4. DIVISIBILIDADE EM $A[x]$

### 4.1 Divisão exata

Dados $f, g \in A[x]$, diz-se que um polinômio $f$ *divide* $g$ se existe um polinômio $h \in A[x]$ tal que $g = fh$. Também se diz, neste caso, que $f$ é *divisor* de $g$ ou que $g$ é *divisível* por $f$. Para indicar essa relação usa-se a notação $f \mid g$. Se $f$ não é divisor de $g$, isso é indicado por $f \nmid g$.

Convém observar que, se $f \mid g$, então $g = fq$ e, portanto, $\partial(g) = \partial(f) + \partial(q)$. Em particular $\partial(f) \leq \partial(g)$.

*Exemplo 6:* Em $\mathbb{R}[x]$ o polinômio $x - 1$ divide o polinômio $x^2 - 1$, pois

$$x^2 - 1 = (x - 1)(x + 1)$$

De modo geral, $(x - u) \mid (x^n - u^n)$, devido à identidade demonstrada neste capítulo, em **3.1**.

*Exemplo 7.* Em qualquer anel $A[x]$, os polinômios constantes não nulos, definidos por elementos inversíveis de $A$, dividem todos os polinômios. De fato, qualquer que seja o polinômio $f$, se $c$ é inversível em $A$, vale a igualdade $f = c\left[\left(\frac{1}{c}\right)f\right]$. Como $\left(\frac{1}{c}\right)f$ pertence ao anel dos polinômios a que pertence $f$, pois $\frac{1}{c}$ pertence ao anel de coeficientes, a afirmação feita fica justificada.

A relação de divisibilidade, definida acima, goza das seguintes propriedades:

- $f \mid f$ (reflexiva).
- Se $f \mid g$ e $g \mid h$, então $f \mid h$ (transitiva).
- Se $f \mid g_1$ e $f \mid g_2$, então $f \mid (g_1h_1 + g_2h_2)$, quaisquer que sejam os polinômios $h_1$ e $h_2$.

Demonstraremos a última dessas propriedades. Por hipótese, existem polinômios $q_1$ e $q_2$ tais que $g_1 = fq_1$ e $g_2 = fq_2$. Daí, $g_1h_1 + g_2h_2 = fq_1h_1 + fq_2h_2 = f(q_1h_1 + q_2h_2)$ e, portanto, $f \mid (g_1h_1 + g_2h_2)$.

Dessa última propriedade saem, como casos particulares, as seguintes propriedades:

- Se $f \mid g_1$ e $f \mid g_2$, então $f \mid (g_1 \pm g_2)$.
- Se $f \mid g$, então $f \mid gh$, qualquer que seja o polinômio $h$.

**Definição 2:** Dois polinômios $f, g \in A[x]$ tais que $f \mid g$ e $g \mid f$ dizem-se *associados*. Quando $f$ e $g$ são associados, diz-se também que $g$ é *associado* de $f$, e vice-versa.

**Proposição 4:** Seja $f \in A[x]$ um polinômio não nulo. Então um polinômio $g \in A[x]$ é associado de $f$ se, e somente se, $g = cf$, para algum polinômio constante inversível $c$.

*Demonstração:*

($\rightarrow$) De fato, por hipótese, $g = fh_1$ e $f = gh_2$, para convenientes polinômios $h_1, h_2 \in A[x]$. Assim:

$$g = g(h_1h_2)$$

e dessa igualdade segue que $h_1h_2 = 1_A$ e, desse modo, $h_1$ e $h_2$ são polinômios inversíveis e, portanto, constantes.

($\leftarrow$) Como $g = cf$, então $f \mid g$. Mas, de $g = cf$, segue que $(c^{-1})g = f$, pois $c$ é inversível. Logo, $g \mid f$ e, portanto, $g$ e $f$ são associados. #

Os associados de um polinômio $f$ e os polinômios inversíveis são chamados *divisores triviais* de $f$.

## 4.2 Algoritmo euclidiano

Observemos os polinômios reais (sobre $\mathbb{R}$) $1 + x^2$ e $1 + x$. Obviamente o primeiro não divide o segundo, já que tem grau maior que este. Mas o segundo

também não divide o primeiro. De fato, se dividisse, existiria um polinômio de grau 1, digamos $a + bx$, tal que $1 + x^2 = (1 + x)(a + bx) = a + bx + ax + bx^2 = a + (a + b)x + bx^2$. Pelo princípio de identidade de polinômios:

$$a = 1, a + b = 0 \text{ e } b = 1$$

Como obviamente isso é impossível, então $1 + x$ não divide $1 + x^2$.

Veremos, porém, que sob certas condições, é possível conseguir uma "divisão aproximada" de um polinômio por um outro — tal como acontece no anel $\mathbb{Z}$.

**Proposição 5** (algoritmo euclidiano): Dados os polinômios $f, g \in A[x]$, com $g \neq 0$ e o coeficiente dominante de $g$ inversível, então existem polinômios $q$ e $r$ tais que $f = gq + r$, em que ou $r = 0$ ou $\partial(r) < \partial(g)$. Ademais, é único o par de polinômios $(q, r)$ que cumpre as condições da proposição.

*Demonstração:*

(Existência)

Para a demonstração suporemos $f(x) = a_0 + a_1x + ... + a_nx^n$ e $g(x) = b_0 + b_1x + ... + b_mx^m$, com $m \geq 0$ e $b_m \neq 0$.

Vamos por casos

(I) $f = 0$ (polinômio identicamente nulo). Neste caso, $q = r = 0$ cumprem as condições do enunciado, pois $0 = g \cdot 0 + 0$.

(II) $f \neq 0$ e $\partial(f) < \partial(g)$. Quando isso acontece, basta tomar $q = 0$ e $r = f$, uma vez que $f = g \cdot 0 + f$ e, por hipótese, $\partial(f) < \partial(g)$.

(III) $f \neq 0$ e $\partial(f) \geq \partial(g)$. Neste caso, procede-se por indução (segundo princípio) sobre o grau de $f$

• Provemos para $\partial(f) = 0$. Quando isso acontece, $\partial(g) = 0$, devido à hipótese. Neste caso, portanto, $f$ e $g$ são polinômios constantes não nulos: $f(x) = a_0$ e $g(x) = b_0$ e $b_0$ é inversível, por hipótese. A divisão recai em $A$, em que é possível e exata: o quociente é $q = b_0^{-1}a_0$ e o resto $r = 0$. De fato, $a_0 = b_0(b_0^{-1}a_0) + 0$.

• Suponhamos agora que $\partial(f) = n > 0$ e que o teorema seja verdadeiro para todo polinômio de grau menor $r$, $0 \leq r < n$.

• Consideremos o polinômio $f_1$ definido da seguinte maneira:

$$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x) \tag{2}$$

Se $f_1 = 0$ ou $\partial(f_1) < \partial(g)$, então $q = a_nb_m^{-1}x^{n-m}$ e $r = f_1$ (para ver isso basta isolar $f(x)$ no primeiro membro).

Caso contrário tem-se $\partial(f_1) \geq \partial(g)$ e $\partial(f_1) < n$, pois o coeficiente dominante de $f$ é igual ao do polinômio expresso por $a_nb_m^{-1}x^{n-m}g(x)$. Portanto, devido à hipótese de indução, existem polinômios $q_1$ e $r_1$ tais que

$$f_1(x) = g(x)q_1(x) + r_1(x), \text{ com } r_1 = 0 \text{ ou } \partial(r_1) < \partial(g) \tag{3}$$

De (2) e (3) segue que

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x)q_1(x) + r_1(x)$$

e, portanto,

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + g(x)q_1(x) + r_1(x),$$

ou

$$f(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)]g(x) + r_1(x)$$

em que $r_1 = 0$ ou $\partial(r_1) < \partial(g)$.

Isso demonstra existência (notar que $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$). #

(Unicidade)

Vamos supor que se pudesse ter $f = gq + r = gq_1 + r_1$, com $\partial(r) < \partial(g)$, se $r \neq 0$, e $\partial(r_1) < \partial(g)$, se $r_1 \neq 0$. Então $g(q - q_1) = r_1 - r$. Como $A[x]$ é um anel de integridade, então $r_1 - r = 0$ se, e somente se, $q - q_1 = 0$ (pois $g \neq 0$).

Suponhamos que $r_1 - r \neq 0$, isto é, $r \neq r_1$, e, portanto, que $q \neq q_1$. Então tem sentido falar no grau de $r_1 - r$ e no de $q - q_1$ e

$$\partial(g(q - q_1)) = \partial(g) + \partial(q - q_1) = \partial(r_1 - r)$$

Logo, $\partial(r_1 - r) \geq \partial(g)$. Mas isso leva sempre a um absurdo. De fato, as possibilidades para $\partial(r_1 - r)$ são as seguintes: (a) $\partial(r_1 - r) = \partial(r_1)$, se $r = 0$, e se teria $\partial(r_1) \geq \partial(g)$, o que é impossível; (b) $\partial(r_1 - r) = \partial(r)$, se $r_1 = 0$, e neste caso se teria $\partial(r) \geq \partial(g)$, o que também não pode ocorrer; (c) $\partial(r_1 - r) \leq$ *máximo* $\{\partial(r_1), \partial(r)\}$, se $r, r_1 \neq 0$, e neste caso se concluiria que *máximo* $\{\partial(r_1), \partial(r)\} \geq \partial(g)$, o que também é impossível.

Logo, $r_1 = r$ e, por conseguinte, $q = q_1$. #

**Corolário:** Seja $K$ um corpo e consideremos $f, g \in K[x]$, com $g \neq 0$. Então existem polinômios $q$ e $r$ tais que $f = gq + r$, em que ou $r = 0$ ou $\partial(r) < \partial(g)$. Ademais, é único o par de polinômios $(q, r)$ que cumpre essas condições.

*Demonstração:* É só observar que, como $K$ é um corpo, o coeficiente dominante de $g$ é necessariamente inversível. #

No algoritmo euclidiano, os polinômios dados, $f$ e $g$, e os polinômios $q$ e $r$, cuja existência e unicidade acabamos de demonstrar, são chamados, respectivamente, *dividendo*, *divisor*, *quociente* e *resto da divisão* de $f$ por $g$.

*Exemplo 8:* Determinemos o quociente e o resto na divisão euclidiana de $f(x) = x^3 - 1$ por $g(x) = x + 3$, ambos em $\mathbb{Z}[x]$.

Como o coeficiente dominante de $g$ é 1, elemento inversível de $\mathbb{Z}$, então a divisão é possível em $\mathbb{Z}[x]$.

Adotemos o seguinte dispositivo:

$$\begin{array}{rrrr|l} x^3 & + 0x^2 & + 0x & - 1 & x + 3 \\ \hline -x^3 & - 3x^2 & & & x^2 \\ \hline & -3x^2 & + 0x & - 1 & \end{array}$$

O polinômio $f_1(x) \quad 3x^2 - 1$ é o primeiro resto parcial, uma vez que seu grau ainda é maior que o de $g$. Aplicar a hipótese de indução a $f_1$ com relação a $g$ significa, na prática, repetir o procedimento usado na etapa anterior. Vejamos:

$$
\begin{array}{rrrr|l}
x^3 & +\,0x^2 & +\,0x & -\,1 & x + 3 \\
\cline{5-5}
-x^3 & -\,3x^2 & & & x^2 - 3x + 9 \\
\hline
 & -3x^2 & +\,0x & -\,1 & \\
 & 3x^2 & +\,9x & & \\
\cline{2-4}
 & & 9x & -\,1 & \\
 & & -9x & -\,27 & \\
\cline{3-4}
 & & & -\,28 &
\end{array}
$$

Logo, o quociente neste caso é $q = 9 - 3x + x^2$ e o resto é $r = -28$.

## Exercícios

**26.** Dividindo o polinômio $f$ por $x^2 - 3x + 5$, obtemos quociente $x^2 + 1$ e resto $3x - 5$. Determine $f$.

**Resolução**

Por definição de divisão, temos: $f \quad qg + r$. Entao:

$f - (x^2 + 1)(x^2 \quad 3x + 5) + (3x \quad 5) - (x^4 \quad 3x^3 + 6x^2 \quad 3x + 5) + (3x \quad 5) - x^4 \quad 3x^3 + 6x^2$

Resposta: $f \quad x^4 \quad 3x^3 + 6x^2$.

**27.** Dados os polinômios $P(x)$ de grau $m$ e $S(x)$ de grau $n (n < m)$, o resto da divisão de $P(x)$ por $S(x)$ tem grau $p$. Determine os possíveis valores de $p$.

**28.** Numa divisão de polinômios em que o dividendo é de grau $p$ e o quociente de grau $q$, qual é o grau máximo que o resto pode ter?

**29.** Efetue a divisão de $f = x^3 + ax + b$ por $g = 2x^2 + 2x - 6$. Qual é a condição para que a divisão seja exata?

**Resolução**

Aplicando o conhecido método da chave, temos:

$$
\begin{array}{rrrr|rrr}
1 & 0 & a & b & 2 & 2 & -6 \\
\cline{5-7}
-1 & -1 & 3 & & \frac{1}{2} & -\frac{1}{2} & \\
\cline{1-4}
 & -1 & a+3 & b & & & \\
 & 1 & 1 & -3 & & & \\
\cline{2-4}
 & & a+4 & b-3 & & &
\end{array}
$$

e o resto é nulo para $a = -4$ e $b = 3$.

Resposta: $q = \frac{1}{2}x - \frac{1}{2}$ e $r = (a + 4)x + (b - 3)$.

Para divisão exata: $a = -4$ e $b \quad 3$.

**30.** Sem efetuar a divisão, determine $a$ e $b$ de modo que o polinômio $f = (x + 2)^3 + (x - 1)^3 + 3ax + b$ seja divisível por $g = (x - 2)^2$.

**Resolução**

Desenvolvendo as potências, obtemos:

$f = 2x^3 + 3x^2 + (15 + 3a)x + (7 + b)$

$g = x^2 - 4x + 4$

Fazendo $q = cx + d$ (pois $\partial q = \partial f - \partial g = 1$) e lembrando que $f = qg$ (pois $f$ é divisível por $g$), temos, para todo $x$:

$2x^3 + 3x^2 + (15 + 3a)x + (7 + b) = (cx + d)(x^2 - 4x + 4) =$

$= cx^3 + (d - 4c)x^2 + (4c - 4d)x + 4d$

Portanto:

$2 = c$

$3 = d - 4c \Rightarrow d = 4c + 3 = 8 + 3 = 11$

$15 + 3a = 4c - 4d \Rightarrow 15 + 3a = 8 - 44 \Rightarrow 3a = -51 \Rightarrow a = -17$

$7 + b = 4d \Rightarrow 7 + b = 44 \Rightarrow b = 37$

Resposta: $a = -17$ e $b = 37$. ■

**31.** Determine os reais $a$ e $b$ de modo que o polinômio $f = x^4 - 3ax^3 + (2a - b)x^2 + 2bx + (a + 3b)$ seja divisível por $g = x^2 - 3x + 4$.

**32.** Dividindo $(x^3 - 4x^2 + 7x - 3)$ por um certo polinômio $p(x)$, obtemos o quociente $(x - 1)$ e o resto $(2x - 1)$. Determine $p(x)$.

**33.** Quais são o quociente e o resto da divisão de $P(x) = x^4 + x^2 + 1$ por $D(x) = x^2 - x + 1$?

**34.** O polinômio $ax^3 + bx^2 + cx + d$ é o quociente da divisão (que é exata) de $x^5 - x^4 - 34x^3 + 34x^2 + 225x - 225$ por $x^2 - 4x + 3$. Determine $|a + b + c + d|$.

**35.** O polinômio real $p(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$ é divisível por $g_1(x) = 2x^2 + \sqrt{5}x$ e por $g_2(x) = x^2 - x - 2$. Quantas são as raízes reais de $p(x)$?

**36.** Para que valores de $m$ o resto da divisão de $P_1(x) = 4x^3 - 3x^2 + mx + 1$ por $P_2(x) = 2x^2 - x + 1$ independe de $x$?

**37.** Sejam $Q$ o quociente e $R$ o resto da divisão de um polinômio $A$ por um polinômio $B$. Dê o quociente e o resto da divisão de $A$ por $2B$.

**38.** Demonstre que, se $f$ e $g$ são polinômios divisíveis por $h$, então o resto $r$ da divisão de $f$ por $g$ também é divisível por $h$.

**Resolução**

Seja $q_1$ o quociente de $f$ por $h$: $f = q_1h$.

Seja $q_2$ o quociente de $g$ por $h$: $g = q_2h$.

Sejam $q$ o quociente e $r$ o resto da divisão de $f$ por $g$: $f = qg + r$.

Temos, então, $r = f - qg = q_1h - qq_2h = (q_1 - qq_2)h$ e, portanto, $r$ é divisível por $h$. ∎

**39.** Mostre que, se $f$ e $g$ são polinômios divisíveis pelo polinômio $h$, então o mesmo ocorre com $f + g$, $f - g$ e $fg$.

**C1.** Para quais valores do natural $n$ o polinômio $f = 1 - x^n + x^{2n} - x^{3n} + x^{4n}$ é divisível pelo polinômio $g = 1 - x + x^2 - x^3 + x^4$?

## 5. SOBRE RAÍZES

### 5.1 O teorema do resto

Inicialmente generalizaremos o conceito de raiz de um polinômio dado na definição 1.

**Definição 3:** Seja $f$ um polinômio sobre $A$ definido por $f(x) = a_0 + a_1x + \dots + a_rx^r$. Suponhamos ainda que $A$ é um subanel unitário de um anel de integridade $L$. Um elemento $u \in L$ é chamado *raiz de f* se $f(u) = a_0 + a_1u + \dots + a_ru^r = 0$ (zero de $L$ — aliás, o mesmo de $A$).

Neste caso, diz-se também que $u$ é raiz da equação $f(x) = 0$

*Exemplo 9:* As raízes do polinômio racional (coeficientes racionais) $f(x) = x^2 - 3$ são os números reais $\sqrt{3}$ e $-\sqrt{3}$.

**Proposição 6** (teorema do resto): Seja $f$ um polinômio sobre $A$, de grau $\geqslant 1$. Se $A$ é um subanel unitário do anel de integridade $L$ e $u$ é um elemento de $L$, então o resto da divisão de $f(x)$ por $(x - u)$ em $L[x]$ é $f(u)$.

*Demonstração:* Se o quociente e o resto na divisão de $f$ por $x - u$ em $L[x]$ são, respectivamente, $q$ e $r$, então:

$$f(x) = (x - u)q(x) + r(x) \tag{4}$$

em que $\partial(r) < \partial(x - u) = 1$, se $r \neq 0$. Portanto, se $r \neq 0$, então $\partial(r) = 0$, ou seja, $r$ é constante.

Mas, substituindo-se a variável em (4) por $u$:

$$f(u) = (u - u)q(u) + r(u) = r(u)$$

E, como $r$ é um polinômio constante, então $r(u) = r$. De onde, $r = f(u)$, como queríamos provar. #

Convém observar que na proposição anterior o quociente $q$ pode ser um elemento de $L[x]$ e que seu grau é uma unidade a menos que o do divisor $f$. De fato, como $r = 0$ ou $\partial(r) = 0$, então $\partial(f) = \partial((x - u)q) = \partial(x - u) + \partial(q) = 1 + \partial(q)$ e, portanto, $\partial(q) = \partial(f) - 1$. Ademais, $f$ e $q$ têm o mesmo coeficiente dominante. Para tirar essa conclusão, basta observar que, pelo princípio de identidade de polinômios, o coeficiente dominante de $f$ é igual ao produto do coeficiente dominante de $(x - u)$, que é 1, pelo coeficiente dominante de $q$, uma vez que $r$ é constante.

**Corolário:** Seja $f$ um polinômio sobre $A$, de grau $\geq 1$. Se $A$ é um subanel unitário do anel de integridade $L$ e $u$ é um elemento de $L$, então $(x - u) \mid f$ (em $L[x]$) se, e somente se, $f(u) = 0$.

*Demonstração:*

($\rightarrow$) Se $(x - u) \mid f$, então o resto da divisão de $f$ por $(x - u)$ é 0. Mas esse resto, pela proposição, é $f(u)$. Logo $f(u) = 0$.

($\leftarrow$) Como $f(u)$ é o resto da divisão de $f$ por $(x - u)$ e $f(u) = 0$, por hipótese, então $(x - u) \mid f$. #

*Exemplo 10:* Se $n$ é um número inteiro positivo ímpar, então $x^n + 1$ é divisível por $x + 1$. De fato, $(-1)^n + 1 = (-1) + 1 = 0$.

A determinação do quociente e o resto da divisão de um polinômio $f$ de grau $\geqslant 1$ por um polinômio de grau 1 do tipo $ax - b$, com $a \neq 0$ e inversível em $A$, pode ser feita, no corpo das frações de $A$, a partir da divisão de $f$ por um conveniente polinômio do tipo $x - u$. De fato, se $K$ é o corpo das frações de $A$, o algoritmo euclidiano aplicado em $K[x]$ a $f$ (dividendo) e $x - \frac{b}{a}$ (divisor) leva a

$$f(x) = \left(x - \frac{b}{a}\right)q(x) + f\left(\frac{b}{a}\right)$$

Multiplicando-se o primeiro fator da primeira parcela do segundo membro por $a$ e o segundo por $\frac{1}{a}$, obtém-se:

$$f(x) = (ax - b)\left(\frac{1}{a}\right)q(x) + f\left(\frac{b}{a}\right)$$

Portanto, devido à unicidade garantida pelo algoritmo, o quociente nessa divisão é o produto de $\frac{1}{a}$ pelo quociente da divisão de $f$ por $x - \left(\frac{b}{a}\right)$ e o resto é o mesmo.

*Exemplo 11:* O resto da divisão de $f(x) = x^3 - 2x^2 - 3$ por $2x + 1$ é $f(-1/2) = (-1/2)^3 - 2(-1/2)^2 - 3 = -1/8 - 1/2 - 3 = -29/8$.

**Proposição 7:** Seja $f$ um polinômio sobre $A$. Se $L$ é um anel de integridade do qual $A$ é um subanel unitário e $u_1, u_2, ..., u_r \in L$ são raízes distintas de $f$, então existe um polinômio $q \in L[x]$ de grau $n - r$ tal que

$$f(x) = (x - u_1)...(x - u_r)q(x)$$

*Demonstração:* Deixaremos de fazê-la, considerando que o raciocínio é análogo ao que foi usado na demonstração do corolário da proposição 1. #

## 5.2 O algoritmo de Briot-Ruffini

O algoritmo a ser estudado aqui é um dispositivo prático para efetuar a divisão de um polinômio $f$ de grau $n \geq 1$ por um polinômio do tipo $x - u$. Para facilitar, representaremos $f(x)$ na forma

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n \ (\therefore a_0 \neq 0)$$

em vez de usar a forma padrão. Usaremos também uma representação semelhante para o quociente

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + ... + b_{n-2}x + b_{n-1}$$

Assim, se o resto for indicado por $r$, tem-se a seguinte igualdade:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n = (x - u)(b_0x^{n-1} + b_1x^{n-2} + ... + b_{n-2}x + b_{n-1}) + r = b_0x^n + (b_1 - ub_0)x^{n-1} + ... + (b_{n-1} - ub_{n-2})x + (r - ub_{n-1})$$

Pelo princípio de identidade de polinômios:

$b_0 = a_0$, $b_1 - ub_0 = a_1$ $(\therefore b_1 = ub_0 + a_1)$, ..., $b_{n-1} - ub_{n-2} = a_{n-1}$ $(\therefore b_{n-1} = ub_{n-2} + a_{n-1})$ e $r - ub_{n-1} = a_n$ $(\therefore r = ub_{n-1} + a_n)$

Isso posto, o quociente e o resto podem ser obtidos mediante o dispositivo abaixo, em que o primeiro elemento da terceira linha é $a_0$ e os demais são as somas dos elementos correspondentes da primeira linha com o produto de $u$ pelo elemento da terceira linha e coluna anterior.

| $a_0$ | $a_1$ | $a_2$ | ... | $a_{n-1}$ | $a_n$ | $u$ |
|---|---|---|---|---|---|---|
| | $ub_0$ | $ub_1$ | ... | $ub_{n-2}$ | $ub_{n-1}$ | |
| $a_0 = b_0$ | $ub_0 + a_1 = b_1$ | $ub_1 + a_2 = b_2$ | ... | $ub_{n-2} + a_{n-1} = b_{n-1}$ | $ub_{n-1} + a_n = r$ | |

*Exemplo 12:* A divisão de $x^4 - 1$ por $x - 2$ pode ser efetuada assim:

| 1 | 0 | 0 | 0 | −1 | 2 |
|---|---|---|---|---|---|
| 1 | 2 | 4 | 8 | $15 = r$ | |

Portanto, o quociente é dado por $q(x) = x^3 + 2x^2 + 4x + 8$, e o resto é $r = 15$.

### Exercícios

**40.** Qual é o quociente da divisão de $2x^4 - 5x^3 \quad 10x \quad 1$ por $x \quad 3$?

**41.** Qual é o resto da divisão de $x^4 + x^3 + x^2 + x + 1$ por $x + 1$?

**42.** Determine $a, a \in \mathbb{R}$, de modo que o polinômio $f = ax^3 + (2a - 1)x^2 + (3a - 2)x + 4a$ seja divisível por $g = x - 1$ e, em seguida, obtenha o quociente da divisão.

**43.** Resolva, em $\mathbb{C}$, a equação $x^4 - 5x^2 - 10x - 6 = 0$, sabendo que duas de suas raízes são $-1$ e 3.

**Resolução**

Vamos dividir $P(x) = x^4 - 5x^2 - 10x - 6$ por $(x + 1)(x - 3)$:

| | | | | | |
|---|---|---|---|---|---|
| 1 | 0 | −5 | 10 | −6 | −1 |
| 1 | 1 | −4 | −6 | 0 | 3 |
| 1 | 2 | 2 | 0 | | |

Temos que $P(x) = (x + 1)(x - 3)(x^2 + 2x + 2)$; portanto, as demais raízes vêm de $x^2 + 2x + 2 = 0$, isto é, $x = -1 \pm i$.

Resposta: $S = \{-1, 3, -1 + i, -1 - i\}$.

**44.** O polinômio $P(x) = x^5 - x^4 - 13x^3 + 13x^2 + 36x - 36$ é tal que $P(1) = 0$. Quais as outras raízes de $P(x)$?

**45.** Determine $p$ e $q$ reais de modo que $f = x^2 + (p - q)x + 2p$ e $g = x^3 + (p + q)$ sejam ambos divisíveis por $2 - x$.

**46.** Na divisão do polinômio $5x^5 + ax^3 + bx^2 + 3x + 1$ por $x - 2$, encontrou-se o quociente $5x^4 + cx^3 + dx^2 + ex + 115$. Determine o resto.

**47.** Determine o polinômio $f$ do segundo grau que, dividido por $x$, $x - 1$ e $x - 2$, apresenta restos 4, 9 e 18, respectivamente.

**Resolução**

Seja $f = ax^2 + bx + c$. Temos:

$f(0) = a \cdot 0^2 + b \cdot 0 + c = 4 \Rightarrow c = 4$ (I)

$f(1) = a \cdot 1^2 + b \cdot 1 + c = 9 \Rightarrow a + b + c = 9$ (II)

$f(2) = a \cdot 2^2 + b \cdot 2 + c = 18 \Rightarrow 4a + 2b + c = 18$ (III)

Substituindo-se (I) em (II) e (III) resulta o sistema:

$$\begin{cases} a + b = 5 \\ 4a + 2b = 14 \end{cases}$$

que, resolvido por adição, dá $a = 2$ e $b = 3$.

Resposta: $f = 2x^2 + 3x + 4$.

**48.** Determine o polinômio do 3º grau que se anula para $x = 1$ e que, dividido por $x + 1$, $x - 2$ e $x + 2$, dá restos iguais a 6.

**49.** Aplicando Briot-Ruffini, determine o quociente $q$ e o resto $r$ da divisão de $f = x^3 - x^2 + x - 1$ por $g = (x - 2)(x - 3)$.

**Resolução**

Sejam $q_1$ o quociente e $r_1$ o resto da divisão de $f$ por $x - 2$.

$f = q_1(x - 2) + r_1$ (I)

Sejam $q_2$ o quociente e $r_2$ o resto da divisão de $q_1$ por $x - 3$.

$q_1 = q_2(x - 3) + r_2$ (II)

Substituindo (II) em (I), vem:

$f = [q_2(x - 3) + r_2](x - 2) + r_1 = q_2(x - 2)(x - 3) + [r_2(x - 2) + r_1]$

Assim, $q_2$ é o quociente procurado e $r_2(x - 2) + r_1$ é o resto procurado.

Apliquemos Briot-Ruffini duas vezes:

| | | | | | |
|---|---|---|---|---|---|
| $f \rightarrow$ | 1 | −1 | 1 | −1 | 2 |
| $q_1 \rightarrow$ | 1 | 1 | 3 | 5 ($r_1$) | |

| | | | | |
|---|---|---|---|---|
| $q_1 \rightarrow$ | 1 | 1 | 3 | 3 |
| $q_2 \rightarrow$ | 1 | 4 | 15 ($r_2$) | |

$q = q_2 = x + 4$

$r = r_2(x - 2) + r_1 = 15(x - 2) + 5 = 15x - 25$

Resposta: $q = x + 4$ e $r = 15x - 25$. ■

**50.** Sendo 8 e 6 os restos respectivos da divisão de um polinômio $P(x)$ por $(x - 5)$ e $(x - 3)$, determine o resto da divisão de $P(x)$ pelo produto $(x - 5)(x - 3)$.

**51.** Qual é o coeficiente de $x^3$ no polinômio $P(x)$ do terceiro grau que se anula para $x = -1$ e dividido separadamente por $x - 1$, $x + 2$ e $x + 3$ deixa sempre resto 10?

**52.** É dado o polinômio $f(x) = (a - 1)x^6 + (a + 1)x^5 + (a^2 - 1)x^4 - (2a + 1)x + 12$.

a) Determine $a$ de modo que o quociente da divisão de $f$ por $g(x) = x^2 + 1$ seja do 3º grau.

b) Para esse valor de $a$, calcule o quociente e o resto da divisão de $f$ por $g$.

**53.** Determine o resto e o quociente da divisão de $f = x^n - a^n$ por $g = x - a$.

**Resolução**

$r = f(a) = a^n - a^n = 0$

Aplicando Briot-Ruffini, temos:

| | $n - 1$ zeros | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | ... | 0 | $-a^n$ | $a$ |
| 1 | $a$ | $a^2$ | $a^3$ | ... | $a^{n-1}$ | 0 ($r$) | |

Resposta: $r = 0$ e $q = x^{n-1} + ax^{n-2} + a^2x^{n-3} + ... + a^{n-1}$. ■

**54.** Determine o resto e o quociente da divisão de $f = x^n + a^n$ por $g = x - a$

**Resolução**

$r = f(a) = a^n + a^n = 2a^n$

Aplicando Briot Ruffini, temos:

($n - 1$ zeros)

| 1 | 0 | 0 | 0 | ... | 0 | $a^n$ | $a$ |
|---|---|---|---|---|---|---|---|
| 1 | $a$ | $a^2$ | $a^3$ | ... | $a^{n-1}$ | $2a^n$ ($r$) | |

Resposta: $r = 2a^n$ e $q = x^{n-1} + ax^{n-2} + a^2x^{n-3} + ... + a^{n-1}$ ■

**55.** Determine os restos e os quocientes das divisões de $f$ por $g$ nos seguintes casos:

a) $f = x^4 - 81$ e $g = x + 3$

b) $f = x^4 + 81$ e $g = x - 3$

c) $f = x^5 + 32$ e $g = x - 2$

d) $f = x^5 - 32$ e $g = x + 2$

e) $f = x^6 - 1$ e $g = x - 1$

f) $f = x^6 + 1$ e $g = x + 1$

g) $f = x^5 + 243$ e $g = x - 3$

h) $f = x^5 + 243$ e $g = x + 3$

**56.** Transforme $x^5 - a^5$ num produto de dois polinômios.

**57.** A divisao de $(x^{999} - 1)$ por $(x - 1)$ tem resto $R(x)$ e quociente $Q(x)$. Qual o valor de $R(x)$ e qual o valor de $Q(x)$ para $x = 0$?

**58.** Para quais valores de $n$ o polinômio $x^{2n} - a^{2n}$ é divisível por $x^2 - a^2$?

**59.** Qual o quociente da divisão de $4x^4 + 6x^3 - 7x^2 + 8x - 7$ por $2x + 3$?

**60.** Qual é o resto da divisão de $f = x^8 + 1$ por $g = 2x - 4$?

**61.** Prove que, se um polinômio $f \in A[x]$ é divisível separadamente por $x - a$ e por $x - b$, com $a \in A$ e $b \in A$ e $a \neq b$, então $f$ é divisível por $(x - a)(x - b)$.

**Resolução**

Seja $q$ o quociente da divisão de $f$ por $(x-a)(x-b)$. O resto dessa divisão é $r = mx + n$, pois $\partial(r) < 2$ ou $r = 0$. Temos: $f = (x - a)(x - b)q + (mx + n)$

Como $f$ é divisível por $x - a$, vem: $f(a) = (a - a)(a - b)q(a) + (ma + n) = 0 \quad (1)$

e, sendo $f$ divisível por $x - b$, vem: $f(b) = (b - a)(b - b)q(b) + (mb + n) = 0 \quad (2)$

Resolvendo o sistema (lembrar que $A$ é anel de integridade).

$$\begin{cases} ma + n = 0 & (1) \\ mb + n = 0 & (2) \end{cases}$$

nas incógnitas $m$ e $n$, obtemos $m = n = 0$ e, assim, $r = 0$. ■

**62.** Prove que $(x - 2)^{2n} + (x - 1)^n - 1$ é divisível por $x^2 - 3x + 2$

**63.** Determine $a$ e $b$ em $\mathbb{R}$ de modo que o polinômio $f = x^3 + 2x^2 + (2a - b)x + (a + b)$ seja divisível por $g = x^2 - x$.

**64.** Quais os valores de $a$ e de $b$ para que o polinômio $x^3 + ax + b$ seja divisível por $(x - 1)^2$?

**65.** Prove que $nx^{n+1} - (n + 1)x^n + 1$ é divisível por $(x - 1)^2$

**66.** Determine os números reais $a$ e $b$ e o maior inteiro $m$ tais que o polinômio $x^5 - ax^4 + bx^3 - bx^2 + 2x - 1$ seja divisível por $(x - 1)^m$.

**67.** Determine o quociente e o resto da divisão de $f = x^3 - 5x^2 + 8x - 4$ por $g = (x - 1)(2x - 4)$.

**Resolução**

Vamos dividir $f$ sucessivamente por $x - 1$ e $2x - 4 = 2(x - 2)$:

| | | | | | |
|---|---|---|---|---|---|
| $f \rightarrow$ | 1 | −5 | 8 | −4 | 1 |
| $q_1 \rightarrow$ | 1 | −4 | 4 | $\underbrace{0}_{r_1}$ | |

| | | | | | |
|---|---|---|---|---|---|
| $q_1 \rightarrow$ | 1 | −4 | 4 | 2 |
| $2q_2 \rightarrow$ | 1 | −2 | $\underbrace{0}_{r_2}$ | |

$q = q_2 = \frac{1}{2}(x - 2) = \frac{1}{2}x - 1$ (ver exercício 49)

$r = r_2(x - 1) + r_1 = 0(x - 1) + 0 = 0$ (ver exercício 49)

Resposta: $q = \frac{1}{2}x - 1$ e $r = 0$.

**68.** Um polinômio $f$, dividido por $x + 2$ e $x^2 + 4$, dá restos 0 e $x + 1$, respectivamente. Qual é o resto da divisão de $f$ por $(x + 2)(x^2 + 4)$?

## Exercícios complementares

**C2.** Efetue a divisão euclidiana de $f = x^n - 1$ por $g = x^p - 1$. Qual deve ser a relação entre $n$ e $p$ para que $f$ seja divisível por $g$?

**C3.** No polinômio $f = nx^{n+2} - (n + 2)x^{n+1} + (n + 2)x - n$ faz-se a mudança de variável $x = y + 1$. Determine o polinômio em $y$. Qual é uma raiz (óbvia) desse polinômio? E do polinômio em $x$?

### 5.3 Raízes múltiplas

Dado um polinômio $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in A[x]$, denomina-se *derivada formal* de $f$, e indica-se por $f'$, o seguinte polinômio sobre $A$

$$f'(x) = a_1 + (2 \cdot a_2)x + (3 \cdot a_3)x^2 + \ldots + (n \cdot a_n)x^{n-1}$$

Obviamente a derivada de um polinômio constante é o polinômio nulo e a derivada de um polinômio de grau $n \geq 1$ é um polinômio de grau no máximo $n - 1$.

Dessa definição decorrem as seguintes propriedades, aqui apenas citadas:

(a) Se $f(x)$ e $g(x)$ são polinômios e $h(x) = f(x) + g(x)$, então $h'(x) = f'(x) + g'(x)$

(b) Se $f(x)$ e $g(x)$ são polinômios e $h(x) = f(x) \cdot g(x)$, então $h'(x) = f'(x)g(x) + g'(x)h(x)$.

(c) Se $f(x)$ é um polinômio e $g(x) = [f(x)]^n$, em que $n$ é um inteiro estritamente positivo, então $g'(x) = n \cdot [f(x)]^{n-1} f'(x)$.

Sejam $f$ um polinômio sobre $A$ e $u$ um elemento de $A$. Suponhamos que $u$ seja uma raiz de $f$. Então, como já vimos, $f$ é divisível por $x - u$ e, se $q_1$ é o quociente, então $f(x) = (x - u)q_1(x)$. Nessas condições, se $u$ não é raiz de $q_1$, dizemos que $u$ é uma *raiz simples* de $f(x)$. Mas pode ocorrer de $u$ ser raiz de $q_1$, e nesse caso existe um polinômio $q_2$ tal que $q_1(x) = (x - u)q_2(x)$ e, portanto, $f(x) = (x - u)^2 q_2(x)$. Se $u$ não é raiz de $q_2$, diz-se que $u$ é uma *raiz dupla* de $f(x)$. E assim por diante.

**Definição 4:** Sejam $f$ um polinômio sobre $A$ e $u$ um elemento de $A$. Se existe um número natural positivo $r$ tal que

$$f(x) = (x - u)^r q_r(x)$$

em que $q_r$ é um polinômio com coeficientes em $A$ e $u$ não é raiz de $q_r$, então se diz que $u$ é uma *raiz de multiplicidade* r de $f(x)$. Se $r > 1$, diz-se que $u$ é uma *raiz múltipla* de $f(x)$.

**Proposição 8:** Seja $f$ um polinômio sobre $A$ e $u \in A$ uma raiz de $f$. Para que $u \in A$ seja raiz múltipla de $f$, é necessário e suficiente que $u$ seja uma raiz de $f'$.

($\rightarrow$) Sendo $u$ uma raiz múltipla de $f$, então existe $q_2$ em $A[x]$ tal que

$$f(x) = (x - u)^2 \cdot q_2(x)$$

Por derivação:

$$f'(x) = 2(x - u)q_2(x) + q_2'(x) \cdot (x - u)^2$$

Portanto, $f'(u) = 0$.

($\leftarrow$) Por hipótese, $f'(u) = 0$. Suponhamos, por absurdo, que $u$ fosse raiz simples de $f$. Então:

$$f(x) = (x - u) \cdot q(x)$$

para um certo $q \in A[x]$ tal que $q(u) \neq 0$. Mas a derivada de $f$ é dada por

$$f'(x) = q(x) + (x - u) \cdot q'(x)$$

Para $x = u$:

$$f'(u) = q(u) + (u - u) \cdot q'(u) = q(u)$$

o que é absurdo, pois $f'(u) = 0$ e $q(u) \neq 0$. #

*Exemplo 13:* O polinômio real $f(x) = 1 + x + x^2$ não tem raízes múltiplas. De fato, $f'(x) = 1 + 2x$, cuja única raiz é $-1/2$. Mas $f(-1/2) = 1 - 1/2 + 1/4 = \frac{1}{4}$.

*Exemplo 14:* Seja $K$ um corpo infinito de característica 0. Então, qualquer que seja $n > 0$, $f(x) = -1 + x^n$ não tem raízes múltiplas. De fato, neste caso, $f'(x) = n \cdot x^{n-1}$ cuja única raiz é 0 (zero do corpo $K$). Mas $f(0) = -1 \neq 0$.

Porém, se a característica de $K$ fosse $n$ (e, portanto, $n$ seria um número primo), então 1 (unidade de $A$) seria raiz de $f(x) = -1 + x^n$ e de $f'$, pois, neste caso, $f'(1) = n \cdot 1 = 0$. Logo, seria raiz múltipla.

## Exercícios

**69.** Determine todas as raízes e respectivas multiplicidades dos polinômios de $\mathbb{C}[x]$:

a) $f(x) = 3(x + 4)(x^2 + 1)$

b) $g(x) = 7(2x - 3)^2(x + 1)^3(x - 5)$

c) $h(x) = 4(x - 10)^5(2x - 3) = 4(x - 10)^5(x - 1)$

d) $p(x) = (x^2 + x + 1)^3(7x - 14i)^5$

**70.** Qual é o grau de um polinômio $P(x)$ cujas raízes são 3, 2, $-1$, com multiplicidades 7, 6 e 10, respectivamente?

**Resolução**

$P(x) = k(x - 3)^7(x - 2)^6(x + 1)^{10}$, em que $k \in \mathbb{C}$ e $k \neq 0$

Resposta: grau 23.

**71.** Forme o polinômio cujas raízes são 2, $-3$, $1 + i$ e $1 - i$, com multiplicidade 1.

**72.** Qual é a multiplicidade da raiz 1 do polinômio $x^4 - x^3 - 3x^2 + 5x - 2$?

**73.** Quais são os valores de $a$ e $b$ para que o polinômio $x^4 + (3a - b)x^3 + (2b - 4)x^2 + (ab + 4)x + a + b$ tenha uma raiz dupla igual a zero?

**74.** Qual deve ser o valor de $m$ para que o polinômio $x^3 - (4 + m)x^2 + (4 + 4m)x - 4m$ admita o número 2 como raiz dupla?

**75.** Se $m$ é raiz dupla da equação $x^3 - 75x + 250 = 0$ e $n = -2m$ é a outra raiz, ache $m$ e $n$.

**Resolução**

A equação dada é redutível à forma $(x - m)^2(x + 2m) = 0$, isto é, desenvolvendo:

$x^3 - 3m^2x + 2m^3 = 0$

Portanto, devemos ter:

$3m^2 = 75$ e $2m^3 = 250$ e isso acarreta $m = 5$ e $n = -10$

Resposta: $m = 5$ e $n = -10$

**76.** Mostre que os seguintes polinômios em $\mathbb{C}[x]$ não têm raízes múltiplas:

$f(x) \quad x^4 + x$
$g(x) - x^5 \quad 5x + 1$
$h(x) - x^6 - 1$

## 5.4 Raízes racionais de um polinômio de $\mathbb{Z}[x]$

Consideremos um polinômio $f(x) - a_0 + a_1x + a_2x^2 + ... + a_nx^n$ com coeficentes inteiros, ou seja, $a_0, a_1, ..., a_n \in \mathbb{Z}$. A seguinte proposição é útil em muitas situações.

**Proposição 9:** Mantida a notação das considerações anteriores, se um número racional $u = \frac{r}{s}$, representado na forma irredutível (isto é, mdc$(r, s) = 1$), é raiz de $f$, então $r \quad a_0$ e $s \mid a_n$.

*Demonstração:* Como $f(u) = 0$, então:

$$a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + ... + a_n\left(\frac{r}{s}\right)^n = 0$$

Multiplicando-se ambos os membros por $s^n$:

$$a_0s^n + a_1rs^{n \quad 1} + a_2r^2s^{n-2} + ... + a_{n-1}r^{n-1}s + a_nr^n = 0 \qquad (5)$$

Pondo $s$ em evidência na soma dos primeiros $n$ termos do primeiro membro e passando para o segundo o último termo, temos:

$$s(a_0s^{n-1} + a_1rs^{n \quad 2} + ... + a_{n \quad 1}r^{n-1}) = -a_nr^n$$

Isso mostra que $s \mid a_nr^n$. Como $s$ é primo com $r^n$ (pois é primo com $s$, por hipótese), então $s \mid a_n$.

A demonstração de que $r \mid a_0$ segue a mesma idéia: colocar $r$ em evidência na soma dos $n$ últimos termos de (5), passar $a_0s^n$ para o segundo membro e depois usar o fato de que, se um número inteiro divide um produto de dois fatores e é primo com um deles, então esse número divide o outro. #

Note-se que a recíproca dessa proposição não é verdadeira. De fato, tomando $u = \frac{1}{3}$ e $f(x) = 1 + 3x^2$, por exemplo, vemos que $1 \mid 1$, $3 \mid 3$ e, no entanto, $\frac{1}{3}$ não é raiz de $f$.

**Corolário1:** Se um número inteiro $r$ é raiz do polinômio $f(x) - a_0 + a_1x + a_2x^2 + ... + a_nx^n \in \mathbb{Z}[x]$, então $r$ é um divisor de $a_0$.

**Corolário2:** Se $f(x) \quad a_0 + a_1x + a_2x^2 + ... + x^n \in \mathbb{Z}[x]$, então as eventuais raízes racionais de $f$ são números inteiros divisores de $a_0$.

De fato, se o número racional $u \quad \frac{r}{s}$ é raiz de $f$, então $s \mid 1$ e, portanto, $s \quad \pm 1$. Logo, $\frac{r}{s} = \pm r$ e, portanto, pertence a $\mathbb{Z}$. Pela proposição, $r$ divide $a_0$ e, portanto, o mesmo acontece com $-r$. De onde, $u \mid a_0$. #

*Exemplo 15:* O polinômio $f \in \mathbb{Z}[x]$ definido por $f(x) - 2 + x + x^2$ não tem raízes racionais. De fato, se as tivesse, elas seriam números inteiros divisores de 2. Mas esses divisores são $+1$, $+2$. Como $f(1)$ 4, $f($ 1) - 2, $f(2)$ 8 e $f(-2)$ 4, então efetivamente $f$ nao tem raízes reais.

*Exemplo 16:* Pode-se provar, por exemplo, que $\sqrt{2}$ é um número irracional usando-se o critério dado pela proposição. De fato, $\sqrt{2}$ evidentemente é raiz do polinômio $f(x) = x^2 - 2 = -2 + x^2$. Mas, se $f$ tivesse uma raiz $u \in \mathbb{Q}$, então essa raiz seria um inteiro divisor de $-2$. Logo, $u = \pm 2, \pm 1$. Mas nenhum desses números é raiz de $f$, como é fácil comprovar. Se $f$ não tem raízes racionais e $\sqrt{2}$ é raiz de $f$, então $\sqrt{2}$ é irracional.

Da mesma maneira se demonstra que $\sqrt{p}$ é irracional, qualquer que seja o número primo positivo $p$.

## Exercícios

**77.** Quais são as raízes inteiras da equação $P(x) = x^3 - 9x^2 + 22x$ 24 = 0?

**Resolução**

Lembremos que resolver a equação $P(x) - 0$ significa encontrar as raizes de $P(x,$

Como o coeficiente de $x^3$ e 1, as possíveis raízes inteiras da equaçao sao os divisores de 24, isto é

1, 1 2, 2, 3, 3, 4, 4, 6, 6, 8, 8, 12, 12, 24, 24

Calculando o valor de $P$ nesses números, temos:

$P(1) \neq 0, P($ 1) $\neq 0, P(2) \neq 0$ $P($ 2) $\neq 0, P(3) \neq 0, P($ 3) $\neq 0, P(4) \neq 0, P($ 4) $\neq 0$

Mas $P(6) - 0$.

Dividindo $P$ por x − 6:

| 1 | −9 | 22 | −24 | 6 |
|---|---|---|---|---|
| 1 | −3 | 4 | 0 | |

recaímos na equação $x^2 - 3x + 4 = 0$, cujas raízes são complexas e não inteiras.

Resposta: 6. ■

**78.** Quais as possíveis raízes inteiras da equação $x^3 + 4x^2 + 2x - 4 = 0$?

**79.** Quais as raízes da equação $3x^3 - 13x^2 + 13x - 3 = 0$?

**80.** Resolva a equação $15x^3 + 7x^2 - 7x + 1 = 0$.

**81.** Resolva a equação $5x^3 - 37x^2 + 90x - 72 = 0$, sabendo que admite raízes inteiras.

**82.** Resolva a equaçao $2x^4 - 5x^3 - 2x^2 - 4x + 3 = 0$.

**Resolução**

Vamos inicialmente pesquisar raízes racionais da equação. Se $\frac{p}{q}$ é raiz, então $p \in \{1, -1, 3, -3\}$ e $q \in \{1, 2\}$.

Portanto, $\frac{p}{q} \in \left\{1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}\right\}$.

Fazendo $P(x) = 2x^4 - 5x^3 - 2x^2 - 4x + 3$, temos:

$P(1) \neq 0, P(-1) \neq 0, P(-3) \neq 0$

Mas $P(3) = 0$ e $P\left(\frac{1}{2}\right) = 0$; portanto, $P$ é divisível por $(x - 3)\left(x - \frac{1}{2}\right)$:

| 2 | −5 | −2 | −4 | 3 | 3 |
|---|---|---|---|---|---|
| 2 | 1 | 1 | −1 | 0 | 1/2 |
| 2 | 2 | 2 | 0 | | |

e recaímos em $2x^2 + 2x + 2 = 0$, cujas raízes são:

$\frac{-2 \pm \sqrt{4 - 16}}{4} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$

Resposta: $S = \left\{3, \frac{1}{2}, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}$ ■

**83.** Determine as raízes da equação $x^5 \quad 8x^3 + 6x^2 + 7x \quad 6 \quad 0$

**84.** Resolva a equação $x^5 \quad x^4 - 82x^3 \quad 281x^2 - 279x \quad 198 \quad 0$.

**85.** Resolva: $2x^6 + x^5 - 13x^4 + 13x^2 - x - 2 = 0$.

**86.** Determine as raízes da equaçao $x^6 + 3x^5 - 6x^4 \quad 6x^3 + 9x^2 + 3x \quad 4 = 0$

**87.** Prove que, se uma equação polinomial de coeficientes inteiros admite como raiz o número irracional $a + \sqrt{b}$, com $a, b \in \mathbb{Z}$, $b$ primo positivo, então $a - \sqrt{b}$ também é raiz.

**88.** Com base no exercício anterior, determine um polinômio com coeficientes inteiros e grau mínimo que tenha como raízes 1, 2 e $1 - \sqrt{2}$.

**89.** Encontre as raízes do polinômio $3x^4 - 5x^3 - 7x^2 + 3x + 2$, sabendo que uma delas é $1 + \sqrt{2}$.

## 5.5 Raízes complexas de um polinômio de $\mathbb{R}[x]$

O primeiro matemático a lidar intencionalmente com números complexos, mas, mesmo assim, entendendo talvez que se tratasse de um desafio inútil, foi o italiano Girolamo Cardano (1501 1576). Até então esses números, quando apareciam (por

exemplo em problemas do segundo grau), eram descartados de pronto, pois nada se sabia sobre sua natureza ou utilidade. Cardano tinha, porém, razões mais fortes para pelo menos matutar sobre esses novos entes matemáticos, devido a seu trabalho com equações cubicas (grau 3), em cuja discussão, como logo se veria, eles têm um papel fundamental. De todo modo, parece que foi Cardano o primeiro matemático a perceber que, na resolução de equações, esses números aparecem "aos pares". Naturalmente em polinômios com coeficientes reais, os únicos concebíveis na época.

Antes de enunciar a proposição seguinte, lembremos que o *conjugado* de um número complexo $z = a + bi$ é o número complexo $\bar{z} = a - bi$. Lembremos ainda as seguintes propriedades, aliás de verificação direta:

- $z = w$ se, e somente se, $\bar{z} = \bar{w}$.
- $\overline{z + w} = \bar{z} + \bar{w}$.
- $\overline{zw} = \bar{z}\,\bar{w}$.
- Se $z$ é um número real, então $\bar{z} = z$.

**Proposição 10:** Seja $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ um polinômio sobre $\mathbb{R}$ Se o número complexo $z$ é raiz de $f$, então $\bar{z}$ também é raiz desse polinômio.

*Demonstração:* Por hipótese:

$$f(z) = a_0 + a_1z + a_2z^2 + ... + a_nz^n = 0$$

Então, levando se em conta as propriedades lembradas:

$$f(\bar{z}) = a_0 + a_1\bar{z} + a_2(\bar{z})^2 + ... + a_n(\bar{z})^n = \bar{a_0} + \bar{a_1}\,\bar{z} + \bar{a_2}\,(\overline{z^2}) + ... + \bar{a_n}\,(\overline{z^n}) =$$
$$= \overline{a_0 + a_1z + a_2z^2 + ... + a_nz^n} = \bar{0} = 0$$

*Exemplo 17.* Encontrar as raízes de $f(x) = -1 + 2x - x^2 + 2x^3$. Inicialmente vejamos se esse polinômio tem raízes racionais. As possíveis, devido à proposição 9, são $1/1 = 1$, $1/-1 = -1$, $1/2$ e $-1/2$. Uma verificação direta mostra que a única raiz racional é $1/2$. As demais são raízes do quociente de $f$ por $(x - 1/2)$. Esse quociente, que pode ser determinado pelo algoritmo de Briot-Ruffini, é $2x^2 + 2$, que tem discriminante $-16$, e, portanto, suas raízes são números complexos conjugados:

$$2x^2 + 2 = 0 \Leftrightarrow x^2 = -1 \Leftrightarrow x = \pm i$$

Então as raízes de $f$ são: $1/2$, $\pm i$.

Uma conseqüência da proposição 10 é que, por exemplo, um polinômio real de grau 3 ou tem uma raiz real ou três raízes reais, nunca duas ou nenhuma. Isso significa que o gráfico de uma função polinomial de grau 3 corta necessariamente o eixo das abcissas, e o faz em um ou três pontos. Por exemplo, o gráfico da função polinomial do exemplo anterior corta o eixo das abcissas apenas no ponto $(1/2, 0)$.

Esse resultado pode ser generalizado para graus ímpares: uma função polinomial real de grau 5 sempre corta o eixo das abcissas, e o faz em um, três ou cinco pontos E assim por diante.

Com uma equação polinomial de grau par pode acontecer de o gráfico não cortar o eixo dos $x$. Mas, quando corta, o número de vezes é par. Por exemplo, $f(x) = x^4 - 1$ corta o eixo das abscissas nos pontos $(1, 0)$ e $(-1, 0)$.

## Exercícios

**90.** Obtenha os polinômios reais de grau mínimo que têm como raízes $i$, $2i$ e $3i$

**Resolução**

Todo polinômio com coeficentes reais que admite a raiz complexa $z$ também admite a raiz $\bar{z}$, portanto, as raízes do polinômio procurado são: $i$, $-i$, $2i$, $-2i$, $3i$ e $-3i$.

O polinômio é:

$k(x - i)(x + i)(x - 2i)(x + 2i)(x - 3i)(x + 3i)$

$k(x^2 + 1)(x^2 + 4)(x^2 + 9)$

Resposta: $k(x^6 + 14x^4 + 49x^2 + 36)$, com $k \neq 0$.

**91.** Os números complexos $1 + i$, $1 + i^2$ e $2 - i$ são raízes do polinômio $p$ com coeficientes reais. O que se pode afirmar sobre o grau de $p$?

**92.** Resolva a equação $x^4 - 4x^2 + 8x + 35 = 0$, sabendo que uma das raízes é $2 + i\sqrt{3}$.

**Resolução**

Como a equação tem todos os coeficientes reais, resulta que outra raiz é $2 - i\sqrt{3}$ (conjugada de $2 + i\sqrt{3}$). Assim, o polinômio dado é divisível por $\left(x - 2 - i\sqrt{3}\right)\left(x - 2 + i\sqrt{3}\right)$, isto é, por $x^2 - 4x + 7$:

$$
\begin{array}{rl|l}
x^4 + 0x^3 - 4x^2 + 8x + 35 & & x^2 - 4x + 7 \\
\hline
-x^4 + 4x^3 - 7x^2 & & x^2 + 4x + 5 \\
\hline
4x^3 - 11x^2 + 8x + 35 & & \\
-4x^3 + 16x^2 - 28x & & \\
\hline
5x^2 - 20x + 35 & & \\
-5x^2 + 20x - 35 & & \\
\hline
0 & &
\end{array}
$$

A equação dada se escreve:

$(x^2 - 4x + 7)(x^2 + 4x + 5) = 0$

e as raizes de $x^2 + 4x + 5 = 0$ são as que faltam. Portanto:

$$x = \frac{-4 \pm \sqrt{16 - 20}}{2} = \frac{-4 \pm 2i}{2} = -2 \pm i$$

Resposta: $S = \{2 + i\sqrt{3}, 2 - i\sqrt{3}, -2 + i, -2 - i\}$

**93.** Resolva a equação $x^4 - 2x^3 + 6x^2 + 22x + 13 = 0$, sabendo que uma das raízes é $2 + 3i$.

**94.** A equação $x^3 + mx^2 + 2x + n = 0$, em que $m$ e $n$ são números reais, admite $1 + i$ como raiz. Quais são os valores de $m$ e $n$?

**95.** Resolva a equação $x^7 - x^6 + 3x^5 - 3x^4 + 3x^3 - 3x^2 + x - 1 = 0$, sabendo que $i$ é uma das raízes da equação e tem multiplicidade 3.

**96.** Uma raiz de uma equação do terceiro grau com coeficientes reais é $1 + 2i$ e a soma das demais raízes é $3 - 2i$. Determine as raízes dessa equação.

## 5.6 Fórmula de interpolação de Lagrange

Graficamente, o resultado que vamos mostrar garante, em particular, que, dados $n$ pontos de um plano cartesiano, cujas abcissas são distintas entre si, existe uma função polinomial de grau $n - 1$ cujo gráfico passa por todos esses pontos.

**Proposição 11:** Sejam $a_1, a_2, ..., a_n$ ($n > 1$) elementos de um corpo $K$, distintos entre si. Se $b_1, b_2, ..., b_n$ também pertencem a $K$, então existe $f \in K[x]$, com $\partial(f) = n - 1$, tal que $f(a_1) = b_1, ..., f(a_n) = b_n$.

*Demonstração:* Para cada $i$, $1 \leqslant i \leqslant n$, consideremos o polinômio $q_i$ assim definido:

$$q_i(x) = (x - a_1)...(x - a_{i-1})(x - a_{i+1})...(x - a_n) = \prod_{j \neq i}(x - a_j)$$

É claro que $q_i(a_j) = 0$ sempre que $j \neq i$ e que $q_i(a_i) = \prod_{j \neq i}(a_i - a_j) \neq 0$ (lembrar hipótese sobre os $a_K$).

Como os quocientes $\dfrac{b_i}{q_i(a_i)}$ pertencem a $K$, então o polinômio

$$f(x) = \sum_{i=1}^{n} \frac{b_i}{q_i(a_i)}\, q_i(x) = \sum_{i=1}^{n} b_i \left(\prod_{j \neq i} \frac{x - a_j}{a_i - a_j}\right)$$

pertence a $K[x]$. Para esse polinômio tem-se, por exemplo:

$$f(a_1) = \frac{b_1}{q_1(a_1)}\, q_1(a_1) + \frac{b_2}{q_2(a_2)}\, q_2(a_1) + ... + \frac{b_n}{q_n(a_n)}\, q_n(a_1) = b_1 + 0 + ... + 0 = b_1$$

Analogamente se demonstra que $f(a_2) = b_2$, $f(a_3) = b_3$, ..., $f(a_n) = b_n$ e, portanto, o polinômio $f$ cumpre o proposto no enunciado. #

*Exemplo 18:* Determinar um polinômio real $f$ de grau 2 tal que

$$f(0) = 1,\ f(1) = 0 \text{ e } f(2) = 1$$

Seguindo os passos da demonstração, que é construtiva, temos:

$$q_1(x) = (x - 1)(x - 2) \therefore q_1(0) = (0 - 1)(0 - 2) = 2$$
$$q_2(x) = (x - 0)(x - 2) \therefore q_2(1) = (1 - 0)(1 - 2) = -1$$
$$q_3(x) = (x - 0)(x - 1) \therefore q_3(2) = (2 - 0)(2 - 1) = 2$$

Logo:

$$f(x) = \frac{1}{2}(x - 1)(x - 2) + \frac{0}{-1}(x - 0)(x - 2) + \frac{1}{2}(x - 0)(x - 1) =$$

$$= \frac{1}{2}(x - 1)(x - 2 + x) = \frac{1}{2}(x - 1)(2x - 2) = (x - 1)^2$$

**Exercícios**

**97.** Determine o polinômio $f$ de grau 3 em $\mathbb{Z}[x]$ tal que $f(1) = -2$, $f(2) = 2$, $f(3) = 14$ e $f(4) = 40$.

**98.** Ache $f \in \mathbb{Q}[x]$ tal que $\partial f = 4$; $f(1) = f(-1) = f(2) = f(-2) = 2$ e $f(0) = 6$.

## 6. POLINÔMIOS IRREDUTÍVEIS

### 6.1 Introdução

Se $K$ é um corpo, os anéis de integridade $K[x]$ apresentam importantes semelhanças algébricas com o anel $\mathbb{Z}$ dos números inteiros. E isso decorre basicamente do fato de que é possível estabelecer neles um algoritmo euclidiano, tal como em $\mathbb{Z}$. O conceito de *polinômio irredutível*, que introduziremos a seguir, corresponde, no anel dos inteiros, ao de número primo. Convém adiantar, contudo, que em situações mais gerais os conceitos "elemento primo" e "elemento irredutível" em um anel de integridade não coincidem, como teremos oportunidade de ver no próximo capítulo.

**Definição 5:** Um polinômio não nulo e não inversível $p \in K[x]$ se diz *irredutível sobre* K se uma decomposição de $p$ num produto de dois fatores de $K[x]$ só for possível com um dos fatores inversível. Ou seja, se $p = fg$, então $f$ é inversível ou $g$ é inversível.

**Proposição 12:** Todo polinômio de grau 1 sobre um corpo $K$ é irredutível.

*Demonstração:* De fato, se $p$ é um polinômio de grau 1 e se $p = fg$, então $\partial(p) = \partial(f) + \partial(g)$. Mas, como $\partial(p) = 1$, então $\partial(f) + \partial(g) = 1$. Como essa igualdade só é possível se $\partial(f) = 1$ e $\partial(g) = 0$, ou vice-versa, então ou $f$ ou $g$ é inversível. #

### 6.2 Irredutibilidade sobre um corpo algebricamente fechado

**Definição 6:** Seja $K$ um corpo. Se todo polinômio não constante de $K[x]$ tem pelo menos uma raiz em $K$, diz-se que $K$ é um corpo *algebricamente fechado.*

*Exemplo 19:* O exemplo mais familiar de corpo algebricamente fechado é o corpo $\mathbb{C}$ dos números complexos. A primeira demonstração desse fato foi dada por K. F. Gauss (1777 1855), em 1848. O teorema que assegura esse fato é conhecido como *teorema fundamental da álgebra*. Um passo gigantesco rumo a esse resultado já fora dado pelo próprio Gauss quase cinqüenta anos antes, em 1799, na sua tese de doutoramento, ao demonstrar que todo polinômio real tem pelo menos uma raiz, real ou complexa. Em 1815 e 1816, Gauss deu duas novas demonstrações desse teorema

**Proposição 13:** Um polinômio sobre um corpo $K$ algebricamente fechado é irredutível se, e somente se, tem grau 1.

*Demonstração:* Seja $f \in K[x]$ um polinômio irredutível. Como $K$ é algebricamente fechado, existe $u \in K$ tal que $f(u) = 0$. Logo, $x - u \mid f(x)$ e, portanto, existe $g \in K[x]$ tal que

$$f(x) = (x - u)g(x)$$

Como, porém, $f$ é irredutível, então o polinômio $g$ é constante não nulo, isto é, existe $a \in K$ tal que $g(x) = a$, para todo $x \in K$. Portanto:

$$f(x) = ax - au$$

em que $au$ é constante. Logo, o grau de $f$ é 1.

A recíproca é verdadeira, devido à proposição anterior. #

**Proposição 14:** Seja $K$ um corpo algebricamente fechado e $f$ um polinômio de grau $n \geqslant 1$ sobre $K$ cujo coeficiente dominante denotaremos por $a$. Então podem ser determinados elementos $u_1, u_2, ..., u_n \in K$ tais que

$$f(x) = a(x - u_1)(x - u_2)...(x - u_n)$$

*Demonstração* (por indução sobre $n$):

Se o grau de $f$ é 1, então $f(x) = ax + b$, com $a \neq 0$. Pondo $a$ em evidência, temos:

$$f(x) = a(x - b/a)$$

o que demonstra o teorema para $n = 1$.

Seja $f$ um polinômio de grau $n > 1$ e suponhamos a proposição verdadeira para todo polinômio de grau $n$ 1. Como $K$ é algebricamente fechado, $f$ tem uma raiz $u_1$ em $K$ e, portanto:

$$f(x) = (x - u_1)q(x) \qquad (6)$$

para um conveniente $q \in K[x]$, de grau $n$ 1 e coeficiente dominante igual ao de $f$. Pela hipótese de indução, existem $u_2, u_3, ..., u_n \in K$ tais que

$$q(x) = a(x \quad u_2)(x \quad u_3)...(x \quad u_n) \qquad (7)$$

em que $a$ é o coeficiente dominante de $q$ e, portanto, de $f$.

Substituindo-se (6) em (7):

$$f(x) = a(x - u_1)(x - u_2)...(x - u_n) \quad \#$$

Obviamente os $u_i$ que aparecem na proposição anterior são as raízes (todas) de $f$. Mas é preciso levar em conta a possibilidade de existência de raízes múltiplas. Supondo então que as raízes distintas $f$ sejam $u_{i_1}, u_{i_2}, ..., u_{i_r}$ e que suas multiplicidades sejam, respectivamente, $\alpha_1, \alpha_2, ..., \alpha_r$, então podemos reunir os fatores iguais de $f(x)$, obtendo:

$$f(x) = a(x - u_{i_1})^{\alpha_1}(x - u_{i_2})^{\alpha_2} ... (x - u_{i_r})^{\alpha_r}$$

Por uma questão de uniformidade de linguagem, pode-se dizer que o número de raízes de um polinômio de grau $n$ sobre um corpo algebricamente fechado é $n$, convencionando-se, para isso, que uma raiz de multiplicidade $\alpha_i$ seja contada $\alpha_i$ vezes.

## 6.3 Relações de Girard

Segundo parece, foi Albert Girard (1595-1632) o primeiro matemático a perceber claramente que, com a aceitação dos números negativos e complexos, o número de raízes de um polinômio com coeficientes numéricos é igual ao seu grau. Na realidade, ele prenunciou o fato de que $\mathbb{C}$ é algebricamente fechado, o que seria demonstrado mais de um século e meio depois por Gauss, como comentamos no exemplo 19. Girard, embora francês de nascimento, viveu a maior parte de sua vida na Holanda, onde estudou e serviu como engenheiro militar no exército de Frederico Henrique de Nassau.

Diga-se de passagem que em sua época os números negativos e os números complexos eram entes ignorados ou rejeitados por muitos matemáticos, pois, além de sua natureza ser ainda meio misteriosa, nem sequer se sabia de utilidade para eles. Girard contribuiu para o entendimento dos números negativos ao introduzi-los em geometria, associados a um sentido contrário ao associado aos números positivos.

A visão e a ousadia matemática de Girard fizeram com que seu nome ficasse associado às relações entre coeficientes e raízes de um polinômio. Para descobrir essas relações, ele considerou, falando em linguagem moderna, as funções simétricas elementares de todas as raízes de um polinômio real $f$ de grau $n$. Se as raízes de $f$ são $u_1, u_2, ..., u_n$ (algumas eventualmente complexas), então essas funções são definidas da seguinte maneira:

$$\sigma_1 = u_1 + u_2 + ... + u_n$$
$$\sigma_2 = u_1u_2 + u_1u_3 + ... + u_1u_n + u_2u_3 + ... + u_{n-1}u_n$$
$$..........................................................$$
$$\sigma_n = u_1u_2...u_n$$

O nome *funções simétricas* deriva do fato de essas expressões não se alterarem quando se permutam seus índices de uma maneira qualquer.

É fácil descobrir as relações entre os coeficientes de um polinômio e as funções simétricas elementares nas situações mais simples.

- Se $f(x) = a_2x^2 + a_1x + a_0$ (grau dois), então:

$a_2x^2 + a_1x + a_0 = a_2(x - u_1)(x - u_2) = a_2[x^2 - (u_1 + u_2)x + (u_1u_2)] =$
$= a_2x^2 - a_2(u_1 + u_2)x + a_2(u_1u_2) = a_2x^2 - a_2\sigma_1x + a_2\sigma_2$

Pelo princípio de identidade de polinômios:

$$-a_2\sigma_1 = a_1 \text{ e } a_2\sigma_2 = a_0$$

Portanto:

$$\sigma_1 = -\frac{a_1}{a_2} \quad \text{e} \quad \sigma_2 = \frac{a_0}{a_2}$$

E, daí:

$$f(x) = a_2(x^2 - \sigma_1x + \sigma_2)$$

- Se $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ (grau três), então:

$a_3x^3 + a_2x^2 + a_1x + a_0 = a_3(x - u_1)(x - u_2)(x - u_3) =$
$= a_3[x^3 - (u_1 + u_2 + u_3)x^2 + (u_1u_2 + u_1u_3 + u_2u_3)x - u_1u_2u_3] =$
$= a_3x^3 - a_3(u_1 + u_2 + u_3)x^2 + a_3(u_1u_2 + u_1u_3 + u_2u_3)x - a_3(u_1u_2u_3)$
$= a_3x^3 - a_3\sigma_1x^2 + a_3\sigma_2x - a_3\sigma_3$

Pelo princípio de identidade de polinômios:

$$-a_3\sigma_1 = a_2, \; a_3\sigma_2 = a_1, \; -a_3\sigma_3 = a_0$$

Logo:

$$\sigma_1 = -\frac{a_2}{a_3}, \; \sigma_2 = \frac{a_1}{a_3} \quad \text{e} \quad \sigma_3 = -\frac{a_0}{a_3}$$

De onde:

$$f(x) = a_3(x^3 - \sigma_1x^2 + \sigma_2x - \sigma_3)$$

Seria desnecessariamente trabalhoso estender formalmente esse raciocínio para o caso geral. As relações de Girard para um polinômio $f(x) = a_0 + a_1x + ... + a_nx^n$ de grau $n$ são, como é de esperar, em vista dos casos particulares focalizados:

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \sigma_2 = \frac{a_{n-2}}{a_n}, ..., \sigma_n = (-1)^n \frac{a_0}{a_n}$$

Portanto:

$$f(x) = a_n[x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} - ... + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n]$$

## Exercícios

**99.** Se $a$, $b$, e $c$ são as raízes do polinômio $x^3 - 2x^2 + 3x - 4$, calcule $\frac{1}{a} + \frac{1}{b} + \frac{1}{c}$.

**100.** Se $a, b, c$ e $d$ são as raízes do polinômio $2x^4 - 7x^3 + 9x^2 - 7x + 2$, qual é o valor da expressão:

$$E = \frac{1}{bcd} + \frac{1}{acd} + \frac{1}{abd} + \frac{1}{abc}?$$

**101.** Calcule a soma dos quadrados das raízes do polinômio $x^4 + 5x^3 - 11x^2 + 4x - 7$.

**102.** Resolva a equação $x^4 - 4x^3 - x^2 + 16x - 12 = 0$, sabendo que duas de suas raízes são simétricas em relação à adição.

**Resolução**

Temos:

(I) $r_1 + r_2 + r_3 + r_4 = -\dfrac{a_3}{a_4} = 4$

(II) $r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4 = \dfrac{a_2}{a_4} = -1$

(III) $r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4 = -\dfrac{a_1}{a_4} = -16$

(IV) $r_1r_2r_3r_4 = \dfrac{a_0}{a_4} = -12$

(V) $r_1 + r_2 = 0$ (condição do problema)

Comparando-se (I) e (V), resulta:

$(r_1 + r_2) + r_3 + r_4 = 4 \Rightarrow r_3 + r_4 = 4 \quad$ (VI)

Substituindo-se (V) em (III), resulta:

$r_1r_2\underbrace{(r_3 + r_4)}_{4} + r_3r_4\underbrace{(r_1 + r_2)}_{0} = -16 \Rightarrow r_1r_2 = -4 \quad$ (VII)

Substituindo-se este último resultado em (IV), vem:

$(r_1r_2)r_3r_4 = -12 \Rightarrow -4r_3r_4 = -12 \Rightarrow r_3r_4 = 3 \quad$ (VIII)

De (VI) e (VIII) resulta que $r_3$ e $r_4$ são as raízes da equação $y^2 - 4y + 3 = 0$, isto é, $r_3 = 1$ e $r_4 = 3$.

De (V) e (VII) resulta que $r_1$ e $r_2$ são as raízes da equação $y^2 - 4 = 0$, isto é, $r_1 = 2$ e $r_2 = -2$.

Resposta: $S = \{2, -2, 1, 3\}$.

**103.** Resolva a equação $x^3 - 4x^2 + x + 6 = 0$, sabendo que uma raiz é igual à soma das outras duas.

**104.** Resolva a equação $x^3 - 10x^2 + 31x - 30 = 0$, sabendo que uma raiz é igual à diferença das outras duas

**105.** Resolva a equação $x^3 + 5x^2 - 12x - 36 = 0$, sabendo que uma raiz é igual ao produto das outras duas.

**106.** Resolva a equação $x^3 + 7x^2 - 6x - 72 = 0$, sabendo que a razão entre duas raízes é $\frac{3}{2}$.

**107.** Quais são os valores de $h$ para que o polinômio $x^3 + hx^2 + (2h + 1)x + 1$ admita duas raízes opostas?

**108.** Determine $m$ de modo que o polinômio $x^3 + mx - 2$ tenha uma raiz dupla.

**109.** Resolva a equação $8x^4 - 28x^3 + 18x^2 + 27x - 27 = 0$, sabendo que uma das raízes tem multiplicidade 3.

**110.** A soma de duas raízes da equação $x^4 + 2x^3 + px^2 + qx + 2 = 0$ é $-1$ e o produto das outras duas raízes é 1. Calcule $p$ e $q$ e resolva a equação.

**111.** Determine $p$ e $q$ de modo que o polinômio $x^4 + px^3 + 2x^2 - x + q$ apresente duas raízes inversas entre si e a soma das outras duas raízes seja igual a 1.

## 6.4 Um critério de irredutibilidade

O critério que enunciaremos ajuda bastante em algumas situações "Se o grau de um polinômio $f$ sobre um corpo $K$ é 2 ou 3, então ou $f$ é irredutível sobre $K$ ou tem uma raiz, pelo menos, em $K$". Mostraremos a validade desse critério para o caso de o grau de $f$ ser 3. No caso em que o grau é 2, o raciocínio é análogo.

De fato, suponhamos que $f$ não fosse irredutível. Então $f$ poderia ser decomposto não trivialmente em um produto $f = gq$ em que os fatores têm grau $\geq 1$. Como, por outro lado, $\partial(f) = \partial(gq) = \partial(g) + \partial(q)$ e $\partial(f) = 3$, então:

$$\partial(g) + \partial(q) = 3$$

Ora, isso só é possível se $\partial(g) = 1$ e $\partial(q) = 2$, ou vice-versa. Supondo, por exemplo, que $\partial(g) = 1$, então a expressão que define $g$ é do tipo

$$g(x) = ax + b \ (a \neq 0)$$

Como $-b/a$ (que pertence a $K$) é raiz de $g$, então também é raiz de $f$. #

*Exemplo 20:* O polinômio $f(x) = 1 + x + x^3 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$. De fato, as possíveis raízes racionais de $f$ são $\pm 1$ (divisores de 1). Mas $f(1) = 3$ e $f(-1) = -1$. Como não tem nenhuma raiz em $\mathbb{Q}$, então $f$ é irredutível sobre esse corpo.

## 6.5 Polinômios irredutíveis sobre o corpo dos números reais

A proposição 13 garante que os únicos polinômios irredutíveis em $\mathbb{C}[x]$ são os de grau 1, pois $\mathbb{C}$ é algebricamente fechado. O mesmo, porém, não vale em $\mathbb{R}[x]$.

o polinômio $f(x) = x^2 + 1$, por exemplo, é irredutível sobre $\mathbb{R}$. De fato, se não o fosse teria uma raiz em $\mathbb{R}$, devido ao critério anterior. Mas é bem sabido que as raízes de $f$ são $i$ e $-i$, que não são numeros reais. A proposição que segue determina quais polinômios reais são irredutíveis sobre $\mathbb{R}$.

**Proposição 15:** Um polinômio $f \in \mathbb{R}[x]$ é irredutível sobre $\mathbb{R}$ se, e somente se, $\partial(f) = 1$ ou $\partial(f) = 2$ e seu discriminante é menor que zero.

*Demonstração:*

($\rightarrow$) Por hipótese, $f$ é irredutível sobre $\mathbb{R}$. Mas, devido ao teorema fundamental da álgebra, $f$ tem uma raiz $\alpha$ em $\mathbb{C}$. Há então duas possibilidades. Uma delas é $\alpha$ ser um número real. Neste caso, $x - \alpha$ divide $f$ em $\mathbb{R}[x]$, o que equivale a dizer que

$$f(x) = (x - \alpha)q(x)$$

para um conveniente polinômio real $q$. Porém, como $f$ é irredutível, isso obriga $q$ a ser constante não nulo, digamos, $q(x) = c$, para qualquer $x \in \mathbb{R}$. Logo:

$$f(x) = cx - c\alpha$$

o que mostra que $\partial(f) = 1$.

A outra possibilidade é $\alpha$ não ser real, ou seja, $\alpha = a + bi$, com $b \neq 0$. Neste caso, devido à proposição 10, $\overline{\alpha}$ também é raiz de $f$. Então f é divisível em $\mathbb{C}[x]$ por $x - \alpha$ e por $x - \overline{\alpha}$ (em $\mathbb{C}[x]$) e, portanto, por

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - (2a)x + (a^2 + b^2)$$

que é um polinômio com coeficientes reais. Então existe $q \in \mathbb{C}[x]$ tal que

$$f(x) = [x^2 - (2a)x + (a^2 + b^2)]q(x) \qquad (8)$$

Por outro lado, como $x^2 - (2a)x + (a^2 + b^2)$ é um polinômio real, pode-se usar o algoritmo euclidiano em $\mathbb{R}[x]$ para o par formado por esse polinômio, como divisor, e $f$ como dividendo. Se $q_1$ e $r$ são respectivamente o quociente e o resto, então:

$$f(x) = [x^2 - (2a)x + (a^2 + b^2)]q_1(x) + r(x)$$

Mas, lembrando o fato de que $q_1$ e $r$ também pertencem a $\mathbb{C}[x]$ e a unicidade do quociente e do resto, concluímos que $q_1 = q$ e $r = 0$, e assim $q \in \mathbb{R}[x]$. Então, como $f$ é irredutível sobre $\mathbb{R}$, a igualdade (8) implica que o polinômio real $q$ é constante, digamos $q(x) = c$, para algum número real não nulo $c$. Portanto, (8) fica:

$$f(x) = cx^2 - (2ac)x + (a^2 + b^2)c$$

Isso já mostra que o grau de $f$ é 2. Ademais, o discriminante de $f$ é

$$\Delta = (2ac)^2 - 4c(a^2 + b^2)c = -4b^2c^2 < 0$$

uma vez que $b \neq 0$ e $c \neq 0$

($\leftarrow$) Se $\partial(f) = 1$, então, pela proposição 12, $f$ é irredutível sobre $\mathbb{R}$. Se $\partial(f) = 2$, então, como já vimos, ou $f$ tem uma raiz em $\mathbb{R}$ ou é irredutível sobre $\mathbb{R}$. Como não tem raízes em $\mathbb{R}$, pois seu discriminante é menor que zero, então $f$ é irredutível sobre $\mathbb{R}$. #

Consideremos um polinômio $f \in \mathbb{R}[x]$. Indiquemos por $c_1, c_2, ..., c_r$ suas raízes reais e por $\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, ..., \beta_t, \overline{\beta_s}$ suas raízes complexas não reais. Então, pelo que vimos na proposição 14:

$$f(x) = a(x - c_1)(x - c_2)...(x - c_r)(x - \beta_1)(x - \overline{\beta_1})...(x - \beta_s)(x - \overline{\beta_s})$$

que é uma igualdade em $\mathbb{C}[x]$. Observemos, porém, que, fazendo $\beta_1 = a_1 + b_1 i$, temos:

$$(x - \beta_1)(x - \overline{\beta_1}) = x^2 - (2a_1)x + (a_1^2 + b_1^2)$$

Como o discriminante desse polinômio quadrático é

$$(2a_1)^2 - 4 \cdot 1 \cdot (a_1^2 + b_1^2) = -4b_1^2 < 0$$

então ele é irredutível sobre $\mathbb{R}$. O mesmo se verifica obviamente para os demais produtos $(x - \beta_K)(x - \overline{\beta_K})$.

Repetindo esse raciocínio com os demais pares de produtos envolvendo raízes complexas, obtemos:

$$f(x) = a(x - c_1)(x - c_2)...(x - c_r)[x^2 - (2a_1)x + (a_1^2 + b_1^2)]...$$
$$[x^2 - (2a_s)x + (a_s^2 + b_s^2)]$$

em que os fatores são polinômios reais. Essa é a decomposição de $f(x)$ em fatores irredutíveis sobre $\mathbb{R}$. É claro que pode haver fatores iguais, tanto entre os de grau 1 como entre os de grau 2, que poderiam ser reunidos de maneira óbvia.

## 6.6 Sobre a irredutibilidade em $\mathbb{Q}[x]$

Conforme vimos, não há polinômios complexos irredutíveis de grau maior que 1, assim como não há polinômios reais irredutíveis de grau maior que 2. Em $\mathbb{Q}[x]$, porém, a situação é diferente, como mostra o exemplo 20: o polinômio racional $f$ definido por $f(x) = 1 + x + x^3$ é irredutível sobre $\mathbb{Q}$. Mostraremos no próximo capítulo que em $\mathbb{Q}[x]$ existem polinômios irredutíveis sobre $\mathbb{Q}$ de graus arbitrariamente grandes.

### Exercícios

**112.** Decomponha o polinômio $-x^3 + 4x^2 + 7x - 10$ de $\mathbb{Z}[x]$ em um produto de fatores do primeiro grau.

**113.** Decomponha o polinômio $x^4 - 4$ de $K[x]$ em fatores irredutíveis nos seguintes casos.

a) $K = \mathbb{Q}$

b) $K = \mathbb{R}$

c) $K = \mathbb{C}$

**114.** Mostre que o polinômio $4 + x^4$ de $\mathbb{Z}[x]$ é composto.

*Sugestao:* mostre que o polinômio dado não tem raízes inteiras e, portanto, se for composto só pode ser fatorado com fatores $g$ e $h$ de grau 2. Determine $g$ e $h$.

**115.** Mostre que o polinômio $1 + x + x^3 + x^4$ é composto sobre qualquer corpo $K$.

**116.** Represente $f(x) = 1 + x^4$ como um produto de dois polinômios unitários (coeficientes dominantes iguais a 1) de $\mathbb{R}[x]$, ambos de grau 2.

**117.** Prove que o polinômio $2 + 2x + x^4$ do anel $\mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$.

**118.** Prove que o polinômio $1 + x + x^2$ de $\mathbb{R}[x]$ é irredutível sobre $\mathbb{R}$.

**119.** Quais dos seguintes polinômios do anel $\mathbb{Q}[x]$ são irredutíveis sobre $\mathbb{Q}$?

a) $x^2 - x + 1$

b) $x^3 - 2x^2 + x + 15$

c) $x^4 - 4$

d) $x^4 - x + 1$

**120.** Considere o polinômio $f = 4 + 8x^2$.

a) Como elemento de $\mathbb{Z}[x]$ ele é redutível ou irredutível?

b) E como elemento de $\mathbb{R}[x]$?

c) E como elemento de $\mathbb{C}[x]$?

Justifique

**121.** No anel $\mathbb{Z}[x]$, considere o polinômio $f = x^4 + 4x^3 + 7x^2 + ax + 3$. Determine $a \in \mathbb{Z}$ de modo que $f$ seja decomponível num produto de polinômios de grau 2.

## Exercícios complementares

**C1.** Seja $P$ um ideal primo no anel de integridade infinito $A$. Mostre que $P[x]$ é um ideal primo em $A[x]$. Se $M$ é um ideal maximal em $A$, $M[x]$ é maximal em $A[x]$?

**C2.** Seja $K$ um corpo infinito e $u \in K$. Mostre que $M_u = \{f(x) \mid f(u) = 0\}$ é um ideal maximal em $K[x]$ e $K[x]/M_u$ é isomorfo a $K$.

**C3.** Dado $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{C}[x]$, define-se $\bar{f}(x)$ por:
$\bar{f}(x) = \overline{a_0} + \overline{a_1}x + ... + \overline{a_n}x^n$.
Mostre que $u \in \mathbb{C}$ é raiz de $f(x)$ se, e somente se, $\bar{u}$ é raiz de $\bar{f}(x)$.

CAPÍTULO VII

# ANÉIS PRINCIPAIS E FATORIAIS

## 1. NOTA HISTÓRICA

Não é possível falar da álgebra moderna, a álgebra do século XX, sem ressaltar o nome de Amalie Emy Noether (1882-1935), considerada com justa razão a mais importante matemática de sua época.

Emy Noether nasceu em Erlangen (Alemanha), em cuja universidade local seu pai era um respeitado professor. Embora ao final do curso secundário pendesse para o estudo de línguas, acabou estudando conjuntamente matemática e línguas na Universidade de Erlangen, onde era uma das duas mulheres entre os cerca de mil universitários. Esse fato põe em relevo as condições extremamente desfavoráveis que Emy Noether encontrou, no que se refere ao ensino superior, devido à sua condição de mulher Nessa época, as mulheres só podiam assistir a cursos extra-oficia. mente e com a aquiescência do professor, dada raramente. Não obstante, o fato de poder graduar se, o que ocorreu em 1903, representou um avanço em relação a epo cas não muito distantes

Em 1907, Emy doutorou se com uma tese de bom nivel, mas que não prenun ciava o grande papel que ela teria na matemática do século XX. Até 1916, perma neceu em Erlangen, substituindo eventualmente seu pai como docente e trabalhan do em suas pesquisas, das quais resultariam varios artigos. Nesse ano, foi convida da por David Hilbert (1852-1943), a maior figura da matemática mundial na época,

para assessorá-lo em suas pesquisas relativas à teoria da relatividade, na Universidade de Göttingen Entretanto, a despeito do prestígio e do empenho de Hilbert, só em 1922 passou a receber remuneração da Universidade, e mesmo assim muito mo desta, bem inferior à de seus pares do sexo masculino.

Isso, porém, não impediu que sua produção científica fluísse brilhantemente nem tirou seu ânimo para uma de suas atividades preferidas: a orientação de alu nos. Dentre estes, um dos mais notáveis foi o holandês B. L. van der Waerden (1903-1996), autor do primeiro grande tratado de álgebra moderna, publicado em dois volumes no ano de 1930. Reeditada numerosas vezes e traduzida para várias línguas, essa obra teve influência decisiva na difusão da álgebra moderna A propósito, vale acrescentar que boa parte do segundo volume da obra é contribuição de Emy.

Emy Noether era judia, e o nazismo, que se instaurou na Alemanha em 1933, em pouco lhe tiraria o modesto posto acadêmico. Forçada a emigrar, aceitou convite do Bryn Mayr College, da Califórnia, para ser professora visitante, função que exerceu desde o outono de 1933 até sua morte inesperada, em 1935, após complicações decorrentes de uma cirurgia aparentemente bem-sucedida.

Em poucas linhas é impossível falar satisfatoriamente sobre a obra de Noether e sua importância para a matemática. Registremos, porém, sua definição axiomática de anel, dada em 1921, que, embora não tenha sido a primeira da história da matemática, é a que se usa hoje nos textos de álgebra, salvo no que se refere à comutatividade da multiplicação — atualmente não incluída entre os axiomas —, que ela impunha. Também se deve a Emy a definição de ideal hoje aceita. Em homenagem a ela, os anéis de uma certa categoria, de que daremos um exemplo neste capítulo, em **3.1**, recebem o nome de *anéis noetherianos*.

## 2. DIVISIBILIDADE EM UM ANEL DE INTEGRIDADE

### 2.1 Divisão exata em um anel de integridade

Neste capítulo, estenderemos para um anel de integridade qualquer $A$ a relação definida por "$x$ divide $y$", já estudada em duas situações particulares importantes: no anel $\mathbb{Z}$ dos inteiros e no anel $A[x]$ dos polinômios sobre um anel de integridade infinito $A$. Tendo em vista que neste trabalho não fomos além dos polinômios sobre um anel de integridade infinito, subentenderemos $A$ infinito sempre que aparecer em cena o anel $A[x]$.

Se $a$ e $b$ são elementos de $A$ e se $b = ac$, para algum $c \in A$, dizemos que *a divide b* ou que *b é divisível por a* e denotamos essa relação por $a \mid b$ O elemento $c$ que figura nessa definição será indicado por $b/a$ sempre que $a \neq 0$

A relação de *divisibilidade*, definida dessa maneira, goza das seguintes propriedades:

(i) reflexiva;

(ii) transitiva;

(iii) se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$

Em particular, se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$, $a \mid (b - c)$ e $a \mid bd$, para qualquer $d \in A$.

Deixaremos de dar as demonstrações dessas propriedades porque, além de simples, elas formalmente em nada diferem das correspondentes relativas aos casos particulares mencionados no início.

## 2.2 Elementos associados

**Definição 1:** Sejam $a$ e $b$ elementos de um anel de integridade $A$. Diz-se que $a$ é associado de $b$ se $a \mid b$ e $b \mid a$. Essa relação em $A$ será indicada por $a \sim b$.

É fácil provar que $\sim$ é uma relação de equivalência sobre $A$ (ver exercício 3).

*Exemplo 1:* Os polinômios reais $f(x) = 1 + x$ e $g(x) = 2 + 2x$ são associados, uma vez que

$$2 + 2x = 2 \cdot (1 + x) \text{ e } 1 + x = (1/2)(2 + 2x)$$

**Proposição 1:** Para dois quaisquer elementos $a$ e $b$ de $A$ são equivalentes as seguintes afirmações: (i) $a \sim b$; (ii) $\langle a \rangle = \langle b \rangle$; (iii) $b = au$, para um conveniente elemento inversível $u \in A$.

*Demonstração:*

(i) $\rightarrow$ (ii)

Como $a \sim b$, então $b = ac$ e $a = bd$, para convenientes $c, d \in A$.

Seja $x \in \langle a \rangle$. Então existe $r \in A$ tal que $x = ar$. Levando-se em conta que $a = bd$, então $x = b(dr)$, o que mostra que $x \in \langle b \rangle$. Portanto, $\langle a \rangle \subset \langle b \rangle$. Analogamente se demonstra a inclusão contrária.

(ii) $\rightarrow$ (iii)

Como $\langle a \rangle = \langle b \rangle$ e $a \in \langle a \rangle$, então $a = br$, para algum $r$ em $A$. Analogamente, $b = as$ ($s \in A$). Portanto, $a = a(rs)$. Temos duas possibilidades. Se $a = 0$, então $b = 0$ e, neste caso, vale a igualdade $0 = 0 \cdot 1$. Como 1 é inversível, está provada a tese. Se $a \neq 0$, podemos cancelar $a$ na igualdade $a = a(rs)$, obtendo $rs = 1$. Logo, $r$ é inversível, e como $a = br$, está provada a tese também.

(iii) $\rightarrow$ (i)

Da hipótese de que $b = au$, com $u$ inversível, segue direto que $a \mid b$. Da hipótese, segue ainda que $a = bu^{-1}$, em que $u^{-1}$ é um elemento de $A$, visto que $u$ é inversível. De onde, $b \mid a$. #

## 2.3 Elementos primos e irredutíveis

**Definição 2:** Um elemento $p \in A$ se diz primo se: (i) $p \neq 0$; (ii) $p$ não é inversível, (iii) quaisquer que sejam $a, b \in A$, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Por indução, pode-se demonstrar que, se $p$ é primo e $p \mid a_1 a_2 \ldots a_n$ ($n \geq 1$), então $p$ divide um dos fatores.

*Exemplo 2:* Em $\mathbb{Z}[x]$ o polinômio $h$, definido por $h(x) = x$, é primo, porque obviamente cumpre as condições (i) e (ii) da definição, e se $h \mid fg$, com $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ e $g(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s$, então existem $c_0, c_1, ..., c_t \in \mathbb{Z}$ tais que

$$a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ... + a_rb_sx^{r+s} =$$
$$= c_0x + c_1x^2 + c_2x^3 + ... + c_tx^{t+1}$$

Daí segue, pelo princípio de identidade de polinômios, que

$$a_0b_0 = 0$$

Logo, $a_0 = 0$ ou $b_0 = 0$. Na primeira hipótese, $h$ divide $f$; na segunda, $h$ divide $g$.

**Definição 3:** Um elemento $p \in A$ se diz irredutível se: (i) $p \neq 0$; (ii) $p$ não é inversível; (iii) quaisquer que sejam $a, b \in A$, se $p = ab$, então $a$ é inversível (e, portanto, $b \sim p$) ou $b$ é inversível (e, portanto, $a \sim p$).

Por indução, pode-se provar que, se $p$ é irredutível e $p = a_1a_2...a_n$ ($n \geqslant 1$), então $p$ é associado de um dos fatores do segundo membro e o produto dos demais fatores é inversível.

Um elemento $p \in A$ tal que $p \neq 0$, $p$ nao é inversível e $p$ não é irredutível é chamado *redutível* ou *composto*.

*Exemplo 3:* Se $K$ é um corpo infinito, os polinômios de grau 1 sobre $K$ são irredutíveis, como já vimos no capítulo VI.

**Proposição 2:** Todo elemento primo de um anel de integridade é também irredutível.

*Demonstração:* Seja $p \in A$ um elemento primo. Temos de provar apenas a condição (iii) da definição de elemento irredutível. Para tanto, suponhamos $p = ab$, com $a$ e $b$ em $A$. Como $p \mid p$, então $p \mid ab$. Logo, devido à hipótese, $p \mid a$ ou $p \mid b$.

A primeira dessas possibilidades corresponde à existência de um elemento $c \in A$ tal que $a = pc$. Levando-se em conta isso, a igualdade $p = ab$ se transforma em $p = pcb$. Daí, $cb = 1$ (lembrar que estamos num anel de integridade) e, portanto, $c$ é inversível. Sendo assim, como $a = pc$, então $a$ é associado de $p$.

Com a segunda possibilidade, o raciocínio é o mesmo. #

A recíproca dessa proposição não é verdadeira, como veremos no exemplo 5.

## 2.4 Máximo divisor comum

**Definição 4:** Dizemos que um elemento $d \in A$ é *máximo divisor comum* dos elementos $a, b \in A$ se: (i) $d \mid a$ e $d \mid b$; (ii) todo divisor de $a$ e $b$ é divisor de $d$ (ou seja, se $d_1 \in A$ e $d_1 \mid a$ e $d_1 \mid b$, então $d_1 \mid d$).

De maneira óbvia se define *máximo divisor comum* de $n$ ($n \geqslant 2$) elementos de $A$.

É bom frisar ainda que a definição dada não implica a existência de máximo divisor comum de dois ou mais elementos de $A$

**Proposição 3:** Sejam $a$ e $b$ elementos de $A$. Se $d$ é máximo divisor comum de $a$ e $b$, então todo associado de $d$ também o é. Reciprocamente, se $d$ e $d'$ são máximos divisores comuns de $a$ e $b$, então $d \sim d'$.

*Demonstração:*

($\rightarrow$) Seja $d'$ um associado de $d$. Então $d' \mid d$. Como $d \mid a$ e $d \mid b$, então $d' \mid a$ e $d' \mid b$, devido à transitividade da relação de divisibilidade. Portanto, $d'$ também cumpre a primeira condição da definição de máximo divisor comum.

Indiquemos por $c$ um divisor comum de $a$ e $b$. Como $d$ é máximo divisor comum desses elementos, $c \mid d$. Mas $d \mid d'$, pois $d' \sim d$. Portanto, $c \mid d'$.

($\leftarrow$) Se $d$ e $d'$ são máximos divisores comuns de $a$ e $b$, então são divisores desses elementos e, portanto, devido à segunda condição da definição de máximo divisor comum, $d \mid d'$ e $d' \mid d$. #

Obviamente essa situação de mais de um máximo divisor comum não é boa, matematicamente falando. O ideal é que se verifique a unicidade. Por isso, em situações particulares, costuma-se impor uma condição adicional. Por exemplo, no caso do anel dos inteiros, impõe-se que o máximo divisor comum seja positivo. O fato de, por exemplo, mdc $(3, 5) = 1$ no anel $\mathbb{Z}$ já pressupõe a condição adicional a que nos referimos.

**Definição 5:** Dois elementos de $A$ se dizem *primos entre si* se a unidade do anel é máximo divisor comum desses elementos.

Portanto, de modo geral, todos os elementos inversíveis do anel (e só estes) são máximos divisores comuns dos elementos considerados.

*Exemplo 4:* Os polinômios $f, g \in \mathbb{R}[x]$ definidos respectivamente por $f(x) = x$ e $g(x) = 2 + x$ são primos entre si. De fato, se $p \in \mathbb{R}[x]$ é um divisor de $f$ e $g$ também é divisor de $h = g - h$ que é definido por $h(x) = 2$ e é inversível (seu inverso é o polinômio $h_1$ definido por $h_1(x) = 1/2$), então $p$ também é inversível e os polinômios dados são primos entre si.

## 2.5 Anéis quadráticos

Como mencionamos em **2.3**, embora nas situações mais familiares "primo" e "irredutível" sejam conceitos equivalentes, isso não é verdade em geral. Outras situações fora dos padrões clássicos, como, por exemplo, um anel de integridade em que dois elementos não têm máximo divisor comum, também podem acontecer. O breve estudo que faremos a seguir dos chamados *anéis quadráticos* visa, entre outras coisas, dar oportunidade de focalizar essas situações.

Seja $n \neq 1$ um número inteiro *livre de quadrados*. Isso significa que $n$ não é divisível por nenhum quadrado perfeito, salvo o número 1. Isso posto, indicaremos por $\mathbb{Z}[\sqrt{n}]$ o seguinte subconjunto de $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$$

Pode-se mostrar que, para cada $n$ nas condições enunciadas, $\mathbb{Z}[\sqrt{n}]$ é um subanel unitário de $\mathbb{C}$. Portanto, cada $\mathbb{Z}[\sqrt{n}]$ é um anel de integridade em relação às operações de $\mathbb{C}$, naturalmente restritas aos seus elementos. Cada um deles é chamado *anel quadrático*. Em particular, o anel quadrático em que $n = -1$ é chamado *anel dos inteiros de Gauss*.

O estudo aritmético de $\mathbb{Z}[\sqrt{n}]$ depende em boa parte do conceito de *norma* de um elemento do anel. Se $\alpha = a + b\sqrt{n}$ é um elemento de $\mathbb{Z}[\sqrt{n}]$, sua norma, que será indicada por $N(\alpha)$, é definida da seguinte maneira:

$$N(\alpha) = a^2 - b^2 n$$

Dessa definição decorrem as seguintes propriedades:

(i) $N(\alpha) = 0$ se, e somente se, $\alpha = 0$;

(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$;

(iii) $N(1) = 1$;

(iv) $N(\alpha) = \pm 1$ se, e somente se, $\alpha$ é inversível;

(v) Se $N(\alpha)$ é um número inteiro primo $p$, então $\alpha$ é irredutível em $\mathbb{Z}[\sqrt{n}]$.

Vejamos como se demonstram as duas últimas.

*Demonstração de (iv):*

($\Rightarrow$) Por hipótese, $N(\alpha) = a^2 - nb^2 = \pm 1$. Portanto, $(a + b\sqrt{n})(a - b\sqrt{n}) = \pm 1$. Como $a - b\sqrt{n}$ pertence a $\mathbb{Z}[\sqrt{n}]$, então $\alpha = a + b\sqrt{n}$ é inversível nesse anel.

($\Leftarrow$) Como $\alpha$ é inversível, existe $\beta \in \mathbb{Z}[\sqrt{n}]$ tal que $\alpha\beta = 1$. Daí, $N(\alpha\beta) = N(\alpha)N(\beta) = 1$ e, portanto, $N(\alpha)$ divide 1 em $\mathbb{Z}$. De onde, $N(\alpha) = \pm 1$.

*Demonstração de (v):*

Como $N(\alpha) \neq 1$ e $N(\alpha) \neq 0$, então $\alpha \neq 0$ e $\alpha$ não é inversível. Suponhamos $\alpha = \beta\gamma$ em $\mathbb{Z}[\sqrt{n}]$. Daí, $p = N(\beta)N(\gamma)$, igualdade essa em $\mathbb{Z}$. Logo, $N(\beta) = \pm 1$ ou $N(\gamma) = \pm 1$. Ou seja, ou $\beta$ ou $\gamma$ é inversível. #

*Exemplo 5:* O objetivo aqui é dar um exemplo de elemento irredutível e não primo. Diga-se de passagem que não é em todo anel quadrático que ocorre essa situação; ademais, um estudo mais profundo da questão foge às pretensões deste trabalho.

Mostraremos que no anel $\mathbb{Z}[\sqrt{-5}]$ o número 3 é irredutível mas não é primo. Antes, determinemos os elementos inversíveis desse anel. Observemos primeiro que, se $\alpha \in \mathbb{Z}[\sqrt{-5}]$, então $\alpha = a + b\sqrt{-5}$, para convenientes $a, b \in \mathbb{Z}$, e, portanto, $N(\alpha) = a^2 + 5b^2$. Logo, $N(\alpha)$ é um número inteiro positivo e $N(\alpha) = 1$ se, e somente se, $a = \pm 1$ e $b = 0$. Assim, os únicos elementos inversíveis de $\mathbb{Z}[\sqrt{-5}]$ são 1 e $-1$.

Então 3 não é inversível e, obviamente, também não o é o zero do anel. Suponhamos 3 decomposto em $\mathbb{Z}[\sqrt{-5}]$ num produto de dois fatores: $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Passando à norma dos dois membros, temos.

$$9 = (a^2 + 5b^2)(c^2 + 5d^2)$$

Dessa igualdade (em $\mathbb{Z}$) resulta:

$$a^2 + 5b^2 = 1 \text{ ou } 9$$

pois, para quaisquer inteiros $a$ e $b$, $a^2 + 5b^2 \neq 3$. Se $a^2 + 5b^2 = 1$, então $a + b\sqrt{-5}$ é inversível. Se $a^2 + 5b^2 = 9$, então $c^2 + 5d^2 = 1$ e, portanto, $c + d\sqrt{-5}$ é inversível. Isso mostra que 3 é irredutível.

Para mostrar que 3 não é primo, mostraremos que $3 \mid \left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right)$ mas não divide nenhum desses fatores. Quanto à primeira afirmação, basta observar que $\left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right) = 9$ e que, obviamente, $3 \mid 9$. Suponhamos, por absurdo, que 3 dividisse o fator $2 + \sqrt{-5}$, por exemplo. Então $3 = \left(2 + \sqrt{-5}\right)\left(a + b\sqrt{-5}\right)$, para convenientes elementos $a, b \in \mathbb{Z}$. Passando à norma, temos:

$$9 = (2^2 + 5 \cdot 1^2)(a^2 + 5b^2) = 9(a^2 + 5b^2)$$

e, portanto:

$$a^2 + 5b^2 = 1$$

Logo, $a = \pm 1$ e $b = 0$. Temos, pois, duas situações:

$$3 = \left(2 + \sqrt{-5}\right) \cdot 1 = 2 + \sqrt{-5} \text{ ou } 3 = \left(2 + \sqrt{-5}\right) \cdot (-1) = -2 - \sqrt{-5}$$

ambas impossíveis. Então, efetivamente, 3 não é primo em $\mathbb{Z}\left[\sqrt{-5}\right]$.

## Exercícios

**1.** Mostre que a relação definida por "$x \mid y$" em um anel de integridade não é simétrica mas pode ser anti-simétrica.

**2.** Sejam $a$ e $b$ elementos de um anel de integridade $A$. Mostre que $a \mid b$ se, e somente se, $\langle b \rangle \subset \langle a \rangle$.

**3.** Mostre que a relação definida sobre um anel de integridade por "$x \sim y$" ("$x$ é associado de $y$") é uma relação de equivalência.

**4.** Seja $A$ um anel de integridade.

a) Mostre que o zero do anel só tem um associado: ele mesmo.

b) Mostre que, se $u \in A$ é inversível, então o conjunto dos associados de $u$ é $U(A)$. (Lembrar que $U(A)$ indica o conjunto dos elementos inversíveis de $A$.)

**5.** Sejam $a$ e $b$ elementos associados de um anel de integridade $A$. Se $c$ é também um elemento de $A$, mostre que $c \mid a$ se, e somente se, $c \mid b$

**6.** Seja $A$ um anel de integridade. Como $\sim$ é uma relação de equivalência sobre $A$, pode-se cogitar de descrever os elementos do conjunto quociente $A/\sim$.

Descreva-os nos seguintes casos:

a) $A$ é um corpo,

b) $A = \mathbb{Z}$;

c) $A = K[x]$, em que $K$ é um corpo infinito.

**Resolução**

a) Devido ao exercício 4, $\overline{0} = \{0\}$. Por outro lado, como $A$ é um corpo, $U(A) = A^*$. Logo, as classes de equivalência são duas apenas: $\overline{0}$ e $A^*$, esta última igual a $\overline{a}$, qualquer que seja $a \neq 0$ (zero do corpo).

c) Se $f \in K[x]$ há três possibilidades a considerar:

(i) $f = 0$ e, portanto, $\overline{f} = \{0\}$;

(ii) $f \in K^*$ (conjunto dos inversíveis de $K[x]$ e, portanto, $\overline{f} = K^*$;

(iii) $f \notin K$ e, nesse caso, $\overline{f} = \{cf \mid c \in K^*\}$. ■

**7.** Mostre que o polinômio $f$ definido por $f(x) = 2$ é primo em $\mathbb{Z}[x]$ e, portanto, irredutível nesse anel.

*Sugestão:* Se $f \mid gh$, então os coeficientes de $gh$ são pares. Mostrar, por redução ao absurdo, que isso não é possível sem que todos os coeficientes de $f$ ou todos os coeficientes de $g$ sejam pares.

**8.** Considere o anel quadrático $A = \mathbb{Z}\left[\sqrt{-2}\right]$. Mostre que:

a) $U(A) = \{-1, 1\}$;

b) $1 + \sqrt{-2}$ e $1 - \sqrt{-2}$ são elementos irredutíveis em $A$;

c) 3 é um elemento composto do anel.

**Resolução**

a) $\alpha = a + b\sqrt{-2}$ é inversível se, e somente se, $N(\alpha) = a^2 + 2b^2 = 1$. Mas as únicas soluções inteiras para essa equação são $(1, 0)$ e $(-1, 0)$.

Logo, $\alpha = 1$ ou $\alpha = -1$.

b) $N\left(1 + \sqrt{-2}\right) = N\left(1 - \sqrt{-2}\right) = 3$.

c) $3 = \left(1 + \sqrt{-2}\right)\left(1 - \sqrt{-2}\right)$. ■

**9.** Seja $A$ o anel dos inteiros de Gauss.

a) Determine quais das seguintes relações são verdadeiras em $A$: (i) $(1 + i) \mid 2$; (ii) $(2 + 3i) \mid (5 - i)$; (iii) $3 \mid (2 - i)(3 + i)$; (iv) $(3 - 2i) \mid 26$.

b) Mostre que $U(A) = \{1, -1, i, -i\}$.

c) Mostre que $1 + i$, $1 - i$ e 3 são irredutíveis em $A$.

d) Mostre que 2 é um elemento composto do anel $A$.

**10.** Determine todos os divisores em $\mathbb{Z}[i]$ dos seguintes elementos: 2 e $1 + 2i$

**Resolução**

Se $\alpha = a + bi$ é um divisor de 2 em $\mathbb{Z}[i]$, então $2 = \alpha\beta$, para algum $\beta$ do anel. Então $N(2) = 4 = N(\alpha)N(\beta) = (a^2 + b^2)N(\beta)$ e, portanto, $a^2 + b^2 = 1, 2$ ou $4$. A igualdade $a^2 + b^2 = 1$ fornece os divisores inversíveis de $2: 1, -1, i, -i$. As soluções de $a^2 + b^2 = 2$ são $(\pm 1, \pm 1)$, e os valores correspondentes de $\alpha$, ou seja, $1 + i, 1 - i, -1 + i$ e $-1 - i$, devem ser testados; como $1 + i$ é divisor, pois $2 = (1 + i)(1 - i)$, então os demais, que são associados desse elemento, também são divisores de 2; já as soluções inteiras de $a^2 + b^2 = 4$ são $(\pm 2, 0)$ e $(0, \pm 2)$, cujos valores correspondentes de $\alpha$ são $2, -2, 2i$ e $-2i$, todos também divisores de 2 em $\mathbb{Z}[i]$, como é fácil comprovar. Portanto, 2 tem 12 divisores em $\mathbb{Z}[i]$: $1, -1, i, -i$ (inversíveis), $1 + i, 1 - i, -1 + i, -1 - i, 2, -2, 2i$ e $-2i$. ■

**11.** Mostre que o número 1 é um máximo divisor comum de 2 e $1 + 2i$ em $\mathbb{Z}[i]$.
*Sugestão:* Mostre que $1 + 2i$ é irredutível.

**12.** a) Mostre que o conjunto dos elementos inversíveis de $\mathbb{Z}[\sqrt{-3}]$ é $\{-1, +1\}$.
b) Prove que o número 13 é irredutível em $\mathbb{Z}$, inversível em $\mathbb{Q}$ e composto em $\mathbb{Z}[\sqrt{-3}]$.

**13.** Seja $\alpha$ um elemento inversível de um anel quadrático $A$. Mostre que $\alpha, \alpha^2, \alpha^3, \ldots$ são também elementos inversíveis do anel $A$.

**14.** Considere o anel quadrático $A = \mathbb{Z}[\sqrt{2}]$.
a) Determine um elemento inversível $a \in A$ diferente de 1 e $-1$ e o inverso de $\alpha$.
b) Mostre que o conjunto dos elementos inversíveis de $A$ é infinito.

**Resolução**

a) Um elemento $\alpha = a + b\sqrt{2}$ do anel é inversível se, e somente se, $N(\alpha) = a^2 - 2b^2 = \pm 1$. Mas, como o par $(3, 2)$ é solução de $a^2 - 2b^2 = 1$, então $3 + 2\sqrt{2}$ é inversível no anel considerado. ■

**15.** Prove que 3 é composto e, portanto, não é primo em $\mathbb{Z}[\sqrt{-2}]$.

**16.** a) Determine todos os elementos inversíveis de $A = \mathbb{Z}[\sqrt{-11}]$.
b) Mostre que o número 3 é irredutível em $A = \mathbb{Z}[\sqrt{-11}]$ mas não é primo nesse anel.
*Sugestão:* Quanto à segunda parte, observar que $3 \mid (2 + \sqrt{-11})(2 - \sqrt{-11})$.

**17.** Observando que 3 é irredutível em $\mathbb{Z}[i]$ e que $2 = (1 + i)(1 - i)$, em que os fatores são irredutíveis, determine um máximo divisor comum de 3 e 2 no anel

**18.** a) Determine os elementos inversíveis em $\mathbb{Z}[\sqrt{-7}]$.
b) Mostre que os números 2, $1 + \sqrt{-7}$ e $1 - \sqrt{-7}$ são irredutíveis em $\mathbb{Z}[\sqrt{-7}]$.

**19.** a) Determine os elementos inversíveis em $\mathbb{Z}[\sqrt{-17}]$.
b) Mostre que são irredutíveis em $\mathbb{Z}[\sqrt{-17}]$ os seguintes elementos: 2, 3, $1 + \sqrt{-17}$ e $1 - \sqrt{-17}$.

**20.** Mostre que no anel $\mathbb{Z}[\sqrt{-5}]$ os elementos 9 e $6 + 3\sqrt{-5}$ não têm máximo divisor comum.
*Sugestão:* Encontrar os divisores de cada um dos elementos dados (inspirar-se, para isso, no exercício 10) e verificar que nenhum dos divisores comuns cumpre a segunda condição da definição de máximo divisor comum.

**21.** Seja $p$ um número inteiro primo. Mostre que $p$ é irredutível como elemento de $\mathbb{Z}[i]$ se, e somente se, a equação diofantina $x^2 + y^2 = p$ não tem soluções (inteiras).

**Resolução**

($\Rightarrow$) Se a equação tivesse uma solução $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, então $a^2 + b^2 = (a + bi)(a - bi) = p$, em que os fatores do primeiro membro não são inversíveis em $\mathbb{Z}[i]$ (por quê?). Então $p$ seria composto. ■

**22.** Mostre que todo inteiro primo da forma $p = 4n + 3$ é irredutível em $\mathbb{Z}[i]$.
*Sugestão.* Se $a$ é um número inteiro, então $a^2 \equiv 0, 1 \pmod 4$.

## 3. ANÉIS PRINCIPAIS, FATORIAIS E EUCLIDIANOS

### 3.1 Anéis principais

Já demos anteriormente a definição de anel principal. Recordando: trata-se de um anel de integridade cujos ideais são todos principais. Ou seja, se $I$ é um ideal em um anel principal, então existe $a \in I$ tal que $I = \langle a \rangle$. Como já vimos (exemplo 45, capítulo V), o anel $\mathbb{Z}$ é principal. Vale lembrar que a demonstração dessa propriedade depende do algoritmo euclidiano. Também é principal um corpo qualquer. De fato, os únicos ideais em um corpo $K$ são $\{0\} = \langle 0 \rangle$ e $K = \langle 1 \rangle$.

*Contra-exemplo 1:* O anel $\mathbb{Z}[\sqrt{-5}]$ não é principal. Para justificar essa afirmação, mostraremos que o ideal $I = \langle 3, 2 + \sqrt{-5} \rangle$ não é principal nesse anel. Suponhamos que fosse, e indiquemos por $\beta = a + bi$ um eventual gerador de $I$. Então $\langle 3, 2 + \sqrt{-5} \rangle = \langle \beta \rangle$ e, portanto, $\beta \mid 3$ e $\beta \mid (2 + \sqrt{-5})$. Daí, $N(\beta) \mid 9$ e, portanto, $N(\beta) = a^2 + 5b^2 = 1, 3$ ou $9$. Segue, então, que as possibilidades para $\beta$ são: $\pm 1$, $\pm 3$ e $\pm 2 \pm \sqrt{-5}$. Pode se verificar diretamente, contudo, que desses elementos

os únicos divisores comuns a 3 e $2 + \sqrt{-5}$ são $\pm 1$ e, portanto, $\langle 3, 2 + \sqrt{-5} \rangle = \langle 1 \rangle$. Mas isso implica $1 = 3(a + b\sqrt{-5}) + (2 + \sqrt{-5})(c + d\sqrt{-5}) = (3a + 2c - 5d) + (3b + c + 2d)\sqrt{-5}$, para convenientes inteiros $a, b, c$ e $d$. Como, porém, o sistema

$$\begin{cases} 3a + 2c - 5d = 1 \\ 3b + c + 2d = 0 \end{cases}$$

não tem soluções inteiras (por quê?), então $\langle 3, 2 + \sqrt{-5} \rangle = \langle 1 \rangle$ é impossível.

As proposições que seguem justificam o estudo dos anéis principais, pois mostram o quanto eles são, digamos assim, algebricamente "bem comportados".

**Proposição 4:** Em um anel principal todo elemento irredutível é primo.

*Demonstração:* Seja $p$ um elemento irredutível de um anel principal $A$. Portanto, $p \neq 0$ e $p$ não é inversível. Resta-nos mostrar que, se $p \mid ab$, com $a, b \in A$, então $p$ é divisor de um desses fatores.

Para tanto, consideremos o ideal $I = \langle p, a \rangle$ em $A$. Como o anel é principal, existe $d \in I$ tal que $I = \langle p, a \rangle = \langle d \rangle$. Mas $p$ é um dos elementos de $I$ e, portanto, $p = dc$, para um conveniente $c \in A$. Então, devido à irredutibilidade de $p$, ou $d$ é inversível, e, portanto, $c$ é associado de $p$, ou vice-versa.

Suponhamos primeiro que $d$ é inversível, o que tem como conseqüência $\langle d \rangle = A$. Logo, $\langle p, a \rangle = A$ e, portanto, existem $x_0, y_0 \in A$ tais que 1 (unidade de $A$) $= px_0 + ay_0$.

Multiplicando-se por $b$ ambos os membros dessa igualdade:

$$b = p(bx_0) + (ab)y_0$$

Como $p$ é divisor das duas parcelas do segundo membro desta última igualdade, então $p \mid b$.

Consideremos agora o caso em que $c$ é inversível. Como $p = dc$, então $d = pc^{-1}$. Por outro lado, uma vez que $a$ também pertence a $I$, então $a = dq$, para um conveniente $q \in A$. Das duas últimas igualdades decorre que $a = p(qc^{-1})$ e, portanto, $p$ divide $a$. #

**Proposição 5:** Dois elementos quaisquer de um anel principal têm máximo divisor comum nesse anel.

*Demonstração:* Seja $A$ o anel principal e consideremos $a, b \in A$. Indiquemos por $I$ o ideal gerado por $a$ e $b$, isto é, $I = \langle a, b \rangle$. Por hipótese, $I$ é principal e, portanto, existe $d \in I$ tal que $I = \langle a, b \rangle = \langle d \rangle$. Mostremos que $d$ é máximo divisor comum de $a$ e $b$.

(i) Como $a = a \cdot 1 + b \cdot 0$, então $a \in I$. Mas $I$ é gerado por $d$, e então $a = dq$, para algum $d \in I$. Isso mostra que $d \mid a$. Analogamente se demonstra que $d \mid b$.

(ii) Como $d \in I$, existem $x_0, y_0 \in A$ tais que $d = ax_0 + by_0$. Portanto, se $d'$ é um elemento de $A$ que divide $a$ e $b$, então $d' \mid d$. #

A proposição anterior garante que as identidades de Bezout que relacionam aritmeticamente dois inteiros e seu máximo divisor comum (**4.2**, capítulo II) podem ser estendidas para um anel principal arbitrário.

**Corolário 1:** Dois elementos, $a$ e $b$, de um anel principal $A$ são primos entre si se, e somente se, existem elementos $x_0, y_0 \in A$ tais que $ax_0 + by_0 = 1$.

*Demonstração:* De fato, se $a$ e $b$ são primos entre si, então a unidade do anel, aqui indicada simplesmente por 1, é máximo divisor comum desses elementos e, portanto, levando-se em conta o teorema, $1 = ax_0 + by_0$, para convenientes elementos $x_0, y_0 \in A$.

Reciprocamente, se $1 = ax_0 + by_0$, então todo divisor de $a$ e $b$ também é divisor de 1. Como, obviamente, 1 é divisor de $a$ e $b$, então 1 é máximo divisor comum desses elementos e, portanto, eles são primos entre si. #

Convém acrescentar que a proposição e seu corolário 1 podem ser estendidas naturalmente para um número finito qualquer de elementos do anel.

**Corolário 2:** Se $d$ é um máximo divisor comum de $a$ e $b$, com um deles pelo menos não nulo, então $(a/d)$ e $(b/d)$ são primos entre si.

*Demonstração:* De fato, devido à proposição, existem $x_0, y_0 \in A$ tais que $d = ax_0 + by_0$. Daí, como $d \neq 0$, $1 = (a/d)x_0 + (b/d)y_0$. O corolário anterior nos garante então que $(a/d)$ e $(b/d)$ são primos entre si. #

**Proposição 6:** Um elemento $p \neq 0$ de um anel principal $A$ é irredutível (ou primo) se, e somente se, o ideal $\langle p \rangle$ é maximal.

*Demonstração:*

$(\rightarrow)$ Suponhamos $p$ irredutível e consideremos um ideal $I = \langle a \rangle$ em $A$ tal que $\langle p \rangle \subset I$. Como $p$ pertence ao primeiro desses ideais, então pertence também ao segundo e, portanto, $p = aq$, para um conveniente $q \in A$. Sendo $p$ irredutível, necessariamente um dos fatores, $a$ ou $q$, é inversível.

Ora, como para a primeira dessas possibilidades $I = A$ e como para a segunda $I = \langle p \rangle$, então o único ideal que contém $\langle p \rangle$ propriamente é $A$. Logo, $\langle p \rangle$ é maximal.

$(\leftarrow)$ Suponhamos $\langle p \rangle$ maximal. Então $\langle p \rangle \neq A$ e, portanto, $p$ não é inversível. Suponhamos $p = ab$, com os fatores em $A$. Então $\langle p \rangle \subset \langle a \rangle$ e, portanto, $\langle a \rangle = \langle p \rangle$ ou $\langle a \rangle = A$. No primeiro caso, $a \sim p$ e $b$ é inversível; no segundo, $a$ é inversível e, portanto, $b \sim p$. #

Nosso objetivo agora é mostrar que todo elemento não nulo e não inversível de um anel principal pode ser decomposto em um produto de fatores irredutíveis, "univocamente" em certo sentido, a ser explicitado no enunciado da proposição 7. Para isso precisaremos de dois lemas

**Lema 1:** Seja $I_1 \subset I_2 \subset I_3 \subset \ldots$ uma sequência de ideais em um anel principal $A$. Então existe um índice $r \geq 1$ tal que $I_r = I_{r+1} = \ldots$, ou seja, a sequência é estacionária.

*Demonstração:* Para a demonstração precisaremos do fato de que o conjunto $I = \bigcup_{r=1}^{\infty} I_r$ é um ideal em $A$. De fato, se $x, y \in I$, então existem índices $m, n$ tais que $x \in I_m$ e $y \in I_n$. Fazendo $s = \max\{m, n\}$, temos $x, y \in I_s$ e, por conseguinte, $x - y \in I_s$. Logo, $x - y \in I$. De maneira análoga se demonstra que, se $x \in I$ e $a \in A$, então $ax \in I$.

Como $A$ é principal, existe $d \in I$ tal que $I = \langle d \rangle$. O fato de $d$ estar em $I$ implica que existe um índice $r$ tal que $d \in I_r$. Portanto, $I = \langle d \rangle \subset I_r$. Como, obviamente, $I_r \subset I$, então $I = I_r$. É claro, assim, que $I_r = I_{r+1} = \dots$ #

Quando, em um anel com unidade, toda seqüência crescente de ideais (considerada como ordem a inclusão) é estacionária, diz-se que esse anel é *noetheriano*, designação derivada do nome da matemática Emy Noether, de quem falamos na **Nota histórica** do início deste capítulo. Portanto, todo anel principal é noetheriano.

**Lema 2:** Seja $A$ um anel principal. Então todo elemento não inversível $a \in A$ tem um divisor irredutível nesse anel.

*Demonstração:* Se $a = 0$, a demonstração é imediata. Caso contrário, consideremos o ideal $I_0 = \langle a \rangle$. Se esse ideal for maximal, então, devido à proposição 6, $a$ é irredutível.

Se $I_0$ não for maximal, então existe um ideal $I_1 = \langle a_1 \rangle$ em $A$, diferente de $A$, que contém propriamente $I_0$. Ou seja, $I_0 \subset I_1$, $I_0 \neq I_1$ e $I_1 \neq A$. Se $I_1$ for maximal, então $a_1$ é irredutível. Mas, como $\langle a \rangle \subset \langle a_1 \rangle$, então $a_1 \mid a$. Neste caso, $a_1$ é um divisor irredutível de $a$.

Se $I_1$ não for maximal, repete-se o raciocínio, o que levará à conclusão de que existe um ideal $I_2 = \langle a_2 \rangle$ em $A$, diferente de $A$, tal que $\langle a_1 \rangle \subset \langle a_2 \rangle$, $I_2 \neq I_1$. De novo temos pela frente as mesmas duas possibilidades: ou $I_2$ é maximal e $a_2$ é um elemento irredutível que divide $a_1$, e, portanto, também $a$, ou $I_2$ não é maximal.

Mas, devido ao lema anterior, nenhuma seqüência $I_0 \subset I_1 \subset I_2 \subset \dots$ de ideais em $A$ pode ser estritamente crescente. Logo, para um índice $r + 1$ o ideal $I_{r+1} = \langle a_{r+1} \rangle$ será maximal; o elemento $a_{r+1}$ assim obtido é irredutível e divisor de $a_r, a_{r-1}, \dots, a_1, a$. #

**Proposição 7:** Seja $A$ um anel principal. Então todo elemento $a \in A$, não nulo e não inversível, pode ser decomposto em um produto de fatores irredutíveis. Mais: duas decomposições em fatores irredutíveis, do mesmo elemento não nulo e não inversível, têm igual número de fatores e cada fator de uma delas é associado de algum fator da outra.

*Demonstração:*

(i) (Existência da decomposição)

Se $a \in A$ é irredutível, nada a demonstrar. Então suponhamos $a$ composto. Devido ao lema 2, $a$ tem um divisor irredutível $p_1 \in A$, o que garante a existência de

$a_1 \in A$ ($a_1 \neq 0$, $a_1$ não inversível) tal que $a = p_1a_1$. Se o fator $a_1$ for irredutível, demonstração encerrada. Caso contrário, repete-se o raciocínio com $a_1$, e assim se chegará a uma igualdade $a_1 = p_2a_2$, em que os fatores estão em $A$ e $p_2$ é irredutível. Nesta altura, $a = p_1p_2a_2$. Se $a_2$ for irredutível, demonstração encerrada. Caso contrário, repete-se o raciocínio com $a_2$, e assim por diante. Como a alternativa "$a_i$ não é irredutível" não pode se repetir indefinidamente (por quê?), então, numa dada etapa do raciocínio, $a_s = p_s$ é irredutível e, portanto:

$$a = p_1p_2...p_s$$

em que todos os fatores são irredutíveis.

(ii) (Unicidade)

Vamos supor $a = p_1p_2...p_s = q_1q_2...q_t$. Essa igualdade nos diz que $p_1$ divide $q_1q_2...q_t$ e, portanto, uma vez que é primo, divide um dos fatores, digamos $p_1 \mid q_1$. Mas $q_1$ é irredutível e, portanto, seus únicos divisores são, além dos elementos inversíveis, seus associados. Como $p_1$ não é inversível, então $p_1 \sim q_1$. Logo, $q_1 = u_1p_1$, para algum elemento inversível $u_1$. Da hipótese $p_1p_2...p_s = q_1q_2...q_t = (up_1)q_2...q_t$, segue, cancelando-se $p_1$, que $p_2...p_s = (u_1q_2)q_3...q_t$, em que os fatores, em ambos os membros, são elementos irredutíveis. A repetição desse raciocínio levará à conclusão de que $s = r$ (poderíamos ter, por exemplo, numa certa etapa do raciocínio, $1 = q_{s+1}q_{s+2}...q_t$?) e de que, ajeitando-se os índices, se for o caso, $p_2 \sim q_2$, $p_3 \sim$ $\sim q_3$, ... #

## 3.2 Anéis fatoriais

A definição que segue visa pôr em destaque certa categoria de anéis que abrange os anéis principais, conforme a proposição 7.

**Definição 6:** Diz-se que um anel de integridade $A$ é um *anel fatorial* se as seguintes condições se cumprem: (i) Todo elemento $a \in A$, não nulo e não inversível, pode ser escrito como um produto de elementos irredutíveis de $A$. (ii) Se $a = p_1p_2...p_r = q_1q_2...q_s$ são duas fatorações de $a$ em elementos irredutíveis de $A$, então $r = s$ e, para uma conveniente permutação $\pi$ dos índices, $p_i \sim q_{\pi(i)}$ ($i = 1, 2, ..., r$).

Duas decomposições de um mesmo elemento em fatores irredutíveis, conforme o item (ii) da definição, dizem-se *associadas*.

*Exemplo 6:* O anel $\mathbb{Z}$ é fatorial. De fato, o teorema fundamental da aritmética, conforme o enunciamos e provamos no capítulo II, garante que as condições da definição anterior se verificam para os números inteiros estritamente positivos não inversíveis. Se $a \in \mathbb{Z}$ é negativo não inversível, então $a = (-1)(-a)$, em que $-a$ é estritamente positivo e, portanto, $-a$ pode ser decomposto em um produto de números primos estritamemte positivos, de maneira única, salvo quanto à ordem dos fatores. A justificação se completa considerando-se que $-1$ é inversível em $\mathbb{Z}$.

*Exemplo 7.* Um corpo $K$ é um anel fatorial. De fato, não possuindo senão elementos inversíveis, além do zero, não há em $K$ elementos que contrariem a definição.

*Exemplo 8:* Todo anel principal é fatorial, como mostra a proposição 7.

*Contra exemplo 2:* O anel $\mathbb{Z}[\sqrt{-7}]$ não é fatorial. De fato, $8 = 2 \cdot 2 \cdot 2 = (1 + \sqrt{-7})(1 - \sqrt{-7})$ e os fatores $2$, $1 + \sqrt{-7}$ e $1 - \sqrt{-7}$ são irredutíveis no anel (ver exercício 18). Além do mais, é imediato que 2 não é associado nem de $1 + \sqrt{-7}$ nem de $1 - \sqrt{-7}$. Isso mostra que $\mathbb{Z}[\sqrt{-7}]$ não cumpre a condição (ii) da definição 6 e, portanto, que esse anel não é fatorial.

Se $A$ é fatorial, então na decomposição em fatores irredutíveis de um elemento $a \in A$, não nulo e não inversível, pode ocorrer de alguns pares de fatores serem associados. Podemos ter, digamos, dois fatores irredutíveis distintos, mas associados, $p$ e $q$. Neste caso, $q = vp$ (ou vice-versa), para algum elemento inversível $v$. Logo, $pq = vp^2$. Repetindo-se esse raciocínio sempre que dois ou mais fatores irredutíveis sejam associados, a decomposição se apresentará ao fim sob a forma

$$a = up_1^{\alpha_1}p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

em que $u$ é inversível (lembrar que um produto de inversíveis é inversível), $r \geq 1$, os $\alpha_i$ são inteiros positivos e entre os fatores irredutíveis $p_i$ não há associados.

Em certas situações pode ser conveniente decompor dois elementos em fatores irredutíveis do anel de maneira que em ambas figurem os mesmo fatores irredutíveis. Isso é sempre possível recorrendo-se ao uso do expoente nulo. Assim, se um elemento irredutível aparece na primeira decomposição com expoente não nulo e não aparece explicitamente na segunda, nós o inserimos nesta com expoente igual a 0. Com essa convenção, supondo que os elementos sejam $a$ e $b$, podemos escrevê-los assim:

$$a = up_1^{\alpha_1}p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{e} \quad b = vp_1^{\beta_1}p_2^{\beta_2} \dots p_r^{\beta_r} \tag{1}$$

em que $\alpha_i, \beta_i \geqslant 0$.

Seguem algumas propriedades importantes dos anéis fatoriais.

- Vamos mostrar, construtivamente, que dois elementos quaisquer de um anel fatorial têm máximo divisor comum. Justificaremos esse fato apenas para as situações não triviais: dois elementos não nulos e não inversíveis. Indicando-se esses elementos por $a$ e $b$ e supondo-se que suas decomposições em fatores irredutíveis sejam as de (1), então o elemento

$$d = p_1^{\delta_1}p_2^{\delta_2} \dots p_r^{\delta_r}$$

em que $\delta_i = \min\{\alpha_i, \beta_i\}$, é um máximo divisor comum de $a$ e $b$.

De fato, como $\delta_i \leqslant \alpha_i$ e $\delta_i \leqslant \beta_i$, então $d \mid a$ e $d \mid b$.

Por outro lado, se $d' \in A$ e $d' \mid a$ e $d' \mid b$, então:

$$d' = p_1^{\gamma_1}p_2^{\gamma_2} \dots p_r^{\gamma_r}$$

com $\gamma_i \leqslant \alpha_i$ e $\gamma_i \leqslant \beta_i$. Logo, $\gamma_i \leqslant \min\{\alpha_i, \beta_i\}$ e, por conseguinte, $d' \mid d$.

• Se $a$ e $b$ são elementos de um anel fatorial, dos quais um pelo menos não é nulo, e se $d$ é um máximo divisor comum desses elementos no anel, então $a/d$ e $b/d$ são primos entre si. Recorreremos novamente à convençao usada para escrever $a$ e $b$ com os mesmos fatores primos e expressa nas igualdades (1) e à propriedade anterior. Então, se $p_i^{\alpha_i}$ é fator de $a$ e $p_i^{\beta_i}$ é fator de $b$, os fatores respectivos de $d$, $a/d$ e $b/d$ são: $p_i^{\gamma_i}$, em que $\gamma_i = \min\{\alpha_i, \beta_i\}$, $p_i^{\alpha_i - \gamma_i}$ e $p_i^{\beta_i - \gamma_i}$. Mas $\alpha_i - \gamma_i = 0$ ou $\beta_i - \gamma_i = 0$. Portanto, $\min\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = 0$. Como esse mínimo é o expoente de $p_i$ no máximo divisor comum de $a/d$ e $b/d$, então não há efetivamente fatores irredutíveis comuns a esses elementos, o que justifica nossa afirmação de que eles são primos entre si.

• Se dois elementos $a$ e $b$ de um anel fatorial $A$ não são primos entre si, então eles têm um divisor comum irredutível. De fato, com essa suposição, se $d$ indica um máximo divisor comum de $a$ e $b$, então $d \neq 0$ e $d$ não é inversível. Logo, pode ser decomposto em fatores irredutíveis, conforme a definição 6. Qualquer desses fatores irredutíveis é divisor de $a$ e de $b$.

• Se $p$ é irredutível e $p \mid ab$, ou seja, $ab = pq$, para algum $q \in A$, então $p \mid a$ ou $p \mid b$. Com efeito, se decompusermos cada um dos fatores do primeiro membro de $ab = pq$ em fatores irredutíveis, então, pela "unicidade", $p$ deve ser associado de um desses fatores. Se esse fator for fator de $a$, então $p \mid a$, caso contrário $p \mid b$. Isso mostra que em um anel fatorial todo elemento irredutível é primo.

## 3.3 Anéis euclidianos

Introduziremos agora uma categoria especial de anéis principais. A inspiração é o algoritmo euclidiano, que, como já vimos, vale tanto no anel $\mathbb{Z}$ como em qualquer anel $K[x]$, se $K$ é um corpo infinito. Primeiro é preciso generalizar esse algoritmo.

**Definição 7:** Seja $A$ um anel de integridade e suponhamos que se possa definir uma aplicação $d: A^* = A - \{0\} \to \mathbb{N}$ que cumpra as seguintes condições:

(i) Se $a, b \in A^*$, então $d(ab) \geqslant d(a)$.

(ii) Se $a, b \in A$ e $b \neq 0$, então existem $q, r \in A$ (o quociente e o resto, respectivamente) tais que $a = bq + r$, em que $r = 0$ ou $d(r) < d(b)$.

Neste caso, diz-se que $A$ é um *anel* d*-euclidiano* ou, subentendida a aplicação $d$, simplesmente *euclidiano*.

A definição dada não assegura a unicidade do quociente e do resto. Quanto a essa questão, vale o seguinte resultado (ver exercício 29): "Para que o quociente e o resto na condição (ii) da definição sejam únicos, é necessário e suficiente que $d(a + b) \leqslant \max\{d(a), d(b)\}$".

*Exemplo 9:* O anel $K[x]$ quando $K$ é um corpo.

Neste caso, pode-se tomar como $d = \partial: (K[x])^* \to \mathbb{N}$ a função "grau", isto é, a função que associa a cada polinômio não nulo seu grau.

De fato, como já vimos, se $f$ e $g$ são polinômios não nulos, $\partial(fg) = \partial(f) + \partial(g) \geq \partial(f)$. Além disso, se $f, g \in K[x]$ e $g$ não é o polinômio nulo, o algoritmo euclidiano nos garante que existem $q, r \in K[x]$ tais que $f = gq + r$, em que $r = 0$ ou $\partial(r) < \partial(g)$

*Exemplo 10.* O corpo $\mathbb{Q}$, tomando-se como $d$ a função definida por $d(x) = 1$, qualquer que seja $x \in \mathbb{Q}^*$.

De fato, se $a, b \in \mathbb{Q}^*$, então $d(ab) = 1 = d(a)$.

Se $a, b \in \mathbb{Q}$ e $b \neq 0$, então $a = b(a/b) + 0$.

De maneira análoga pode-se transformar todo corpo em um anel euclidiano.

*Exemplo 11:* Mostraremos agora que o anel $\mathbb{Z}[i]$ dos inteiros de Gauss é euclidiano quando se toma como $d$ a função que associa a cada elemento não nulo de $\mathbb{Z}[i]$ (inteiro de Gauss) sua norma. Lembremos primeiro que, se $\alpha = x + yi$ é um inteiro de Gauss, então $N(\alpha) = x^2 + y^2$ e, portanto, $N(\alpha) \geqslant 1$ se $\alpha \neq 0$. Então, se $\alpha$ e $\beta$ são dois inteiros de Gauss não nulos:

$$N(\alpha\beta) = N(\alpha)N(\beta) \geqslant N(\alpha)$$

ou seja, a condição (i) da definição 7 se verifica para a função considerada.

Consideremos $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$. Então $\alpha/\beta = r + si$, em que $r$ e $s$ são números racionais. Tomemos dois inteiros $m$ e $n$ tais que

$$|r - m| \leqslant \frac{1}{2} \quad \text{e} \quad |s - n| \leqslant \frac{1}{2}$$

o que sempre é possível. Usando-se os inteiros m e n, a igualdade $\alpha/\beta = r + si$ pode ser escrita assim:

$$\alpha/\beta = m + ni + (r - m) + (s - n)i$$

Multiplicando-se ambos os membros por $\beta$:

$$\alpha = \beta(m + ni) + \beta[(r - m) + (s - n)i]$$

Fazendo-se $(m + ni) = \kappa$ e $\beta[(r - m) + (s - n)i] = \rho$ a igualdade anterior fica

$$\alpha = \beta\kappa + \rho$$

Notemos, por último, que, se $\rho \neq 0$, então:

$$N(\rho) = N(\beta)N[(r - m) + (s - n)i] = N(\beta)[(r - m)^2 + (s - n)^2] \leqslant N(\beta)(1/4 + 1/4) < N(\beta)$$

Isso completa a justificação.

**Proposição 8:** Todo anel $d$-euclidiano é principal.

*Demonstração:* Seja $A$ um anel euclidiano e consideremos um ideal $I \neq \langle 0 \rangle$ nesse anel. O conjunto $\{d(x) \mid x \in I \text{ e } x \neq 0\}$ é uma parte de N e, portanto, tem um mínimo $d(b)$. Mostraremos que $I = \langle b \rangle$.

Como $b \in I$, então obviamente $\langle b \rangle \subset I$. Para demonstrar a inclusão contrária, seja $x$ um elemento genérico de $I$. Como $b \neq 0$, a condição (ii) da definição de anel

euclidiano, aplicada a $x$ e a $b$, assegura que existem $q, r \in A$ tais que $x = bq + r$, em que $r \neq 0$ ou $d(r) < d(b)$. Daí, $r = x - bq$ e então $r \in I$. Como, dada a escolha de $b$, a alternativa $r \neq 0$ não pode ocorrer, então $x - bq = 0$, $x = bq$ e, portanto, $x \in I$. #

**Corolário:** Todo anel euclidiano é fatorial.

*Exemplo 12:* Se $K$ é um corpo, então $K[x]$ é fatorial, pelo fato de ser euclidiano e, portanto, principal (exemplo 8)

## Exercícios

**23.** Sejam $I = \langle a \rangle$ e $J = \langle b \rangle$ ideais em um anel principal $A$. Se $I + J = \langle d \rangle$, prove que $d$ é um máximo divisor comum de $a$ e $b$.

**24.** Sejam $a$, $b$ e $c$ elementos de um anel principal. Demonstre que:

a) 1 (unidade do anel) é um máximo divisor comum de $a$ e 1;
b) se $d$ é um máximo divisor comum de $a$ e $b$, então $dc$ é um máximo divisor comum de $ca$ e $cb$;
c) se $a \mid bc$ e $a$ e $b$ são primos entre si, então $a \mid c$;
d) se $a$ e $b$, bem como $a$ e $c$, são primos entre si, então $a$ e $bc$ são primos entre si;
e) se $a$ e $b$ são primos entre si e se $a \mid c$ e $b \mid c$, então $ab \mid c$;
f) se $d \neq 0$ é um máximo divisor comum de $a$ e $b$, então $a/d$ e $b/d$ são primos entre si.

**25.** Mostre que o ideal $\langle 5, 1 + 2\sqrt{-6} \rangle$ no anel $\mathbb{Z}[\sqrt{-6}]$ não é principal.

**26.** Exibindo duas decomposições do número 8 em fatores irredutíveis não associados de $\mathbb{Z}[\sqrt{-7}]$, mostre que esse anel não é fatorial. (Observar que a conclusão pura e simples de que $\mathbb{Z}[\sqrt{-7}]$ não é um anel principal poderia ter sido obtida do fato, a ser provado aqui, de que esse anel não é fatorial.)

**27.** Exibindo duas decomposições de 18 em fatores irredutíveis não associados de $\mathbb{Z}[\sqrt{-17}]$, mostre que esse anel não é fatorial e, portanto, não é principal.

**28.** Seja $A$ um anel $d$-euclidiano. Prove que:

a) se $a$ é um elemento não nulo de $A$, então $d(a) \geq d(1)$;
b) se $a, b \in A^*$ são associados, então $d(a) = d(b)$;
c) um elemento não nulo $a \in A$ é inversível se, e somente se, $d(a) = d(1)$.

**29.** Prove que na definição 7 a unicidade do quociente e do resto vale se, e somente se, $d(a + b) \leq \max\{d(a), d(b)\}$.

**Resolução**

($\leftarrow$) Suponhamos que, para o mesmo par de elementos $a$, $b$ ($b \neq 0$), se tenha: $a = bq + r$ ($r = 0$ ou $d(r) < d(b)$) e $a = bq_1 + r_1$ ($r_1 = 0$ ou $d(r_1) < d(b)$), com $r \neq r_1$ e, portanto, $q \neq q_1$. Então: $d(b) \leqslant d((q - q_1)b) = d(r - r_1) \leqslant \max\{d(r), d(-r_1)\} < d(b)$. Absurdo. ■

**30.** Encontre quociente e resto, no anel dos inteiros de Gauss, na "divisão aproximada" de $\alpha$ por $\beta$, nos seguintes casos:

a) $\alpha = 5 - 2i$ e $\beta = 6 + i$;

b) $\alpha = 3 + 15i$ e $\beta = 1 - 3i$.

**31.** Mostre que são euclidianos os anéis $\mathbb{Z}[\sqrt{n}]$ para n = −2, 2 e 3.
*Sugestão:* Escolha como $d\colon (\mathbb{Z}[\sqrt{n}])^* \to \mathbb{N}$ a função definida por $d(\alpha) = N(\alpha)$, e proceda como para o anel dos inteiros de Gauss.

**32.** Encontre quociente e resto, no anel $\mathbb{Z}[\sqrt{2}]$, na "divisão aproximada" de $\alpha$ por $\beta$, conforme o exercício anterior, nos seguintes casos:

a) $\alpha = 4 + 2\sqrt{2}$ e $\beta = 2 + \sqrt{2}$;

b) $\alpha = 4 - \sqrt{2}$ e $\beta = 2 + 2\sqrt{2}$.

**33.** Consideremos o anel $A = \mathbb{Z}[i]$ dos inteiros de Gauss.

a) Mostre que $I = \langle 3 \rangle$ é um ideal maximal em $A$ e que, portanto, $A/I$ é um corpo.

b) Prove que o anel quociente $\mathbb{Z}[i]/I$ é formado de nove elementos.

**Resolução**

b) Seja $\alpha$ um elemento do anel $A$ e consideremos a classe $\alpha + I$. Aplicando-se o algoritmo euclidiano a $\alpha$ e 3: $\alpha = 3\pi + \rho$, em que $\rho = 0$ ou $N(\rho) < N(3) = 9$.
Segue daí que $\alpha + I = \rho + I$ (por quê?); se $N(\rho) = 0$, então $\rho = 0$ e $\rho + I = 0 + I = I$; se $N(\rho) = 1$, então $\rho = \pm 1, \pm i$, elementos que determinam quatro classes distintas entre si e de $I$ (por quê?), se $N(\rho) = 2$, então $\rho = \pm 1 \pm i$, elementos que determinam mais quatro classes distintas entre si e das anteriores (por quê?). E como não há outras possibilidades (por quê?), então o número de classes distintas é nove. ■

**34.** Se $I$ é um ideal em $A = \mathbb{Z}[i]$, mostre que o anel quociente é finito.
*Sugestão:* Generalizar o raciocínio usado na resolução de 33. b

**35.** No anel $\mathbb{Z}[i]$ encontre decomposições em fatores irredutíveis dos números 6 e $9 + 12i$ e, através delas, determine um máximo divisor comum desses números.

**36.** Sejam $a$ e $b$ elementos de um anel de integridade $A$. Um elemento $m \in A$ se diz mínimo múltiplo comum de $a$ e $b$ se: (i) $m$ é múltiplo de $a$ e $b$; (ii) todo multiplo de $a$ e $b$ é múltiplo de $m$. Isso posto, se $a, b$ são elementos de um anel principal, prove que:

a) todo gerador de $\langle a \rangle \cap \langle b \rangle$ é um mínimo múltiplo comum de $a$ e $b$;

b) se $d$ é um máximo divisor comum de $a$ e $b$ e $m$ um mínimo múltiplo comum, então $ab \sim dm$.

**Resolução**

b) Mostraremos que $\langle a \rangle \cap \langle b \rangle = \langle (ab)/d \rangle$, o que é suficiente (por quê?). Se $x \in \langle (ab)/d \rangle$, então $x = [(ab)/d]t$, para algum $t \in A$. Mas, como $d$ é divisor de $b$, então $(b/d)t \in A$ e, portanto, $x = [(ab)/d]t = a[(b/d)t] \in \langle a \rangle$; analogamente se mostra que $x \in \langle b \rangle$. Agora, se $x \in \langle a \rangle$ e $x \in \langle b \rangle$, então $x = at_1 = bt_2$, para convenientes elementos $t_1, t_2 \in A$. Mas, como $d$ é um máximo divisor comum de $a$ e $b$, então $s_1 = a/d$ e $s_2 = b/d$ são primos entre si (exercício 24f). Substituindo $a$ e $b$ em $at_1 = bt_2$ respectivamente por $ds_1$ e $ds_2$, obtemos $ds_1t_1 = ds_2t_2$. Daí, $s_1t_1 = s_2t_2$ e, como $s_1, s_2 \in A$ são primos entre si, então $s_1 \mid t_2$ (exercício 24c). Se $t_2/s_1 = k$, então $t_2 = s_1k$ e, portanto, $x = bt_2 = bs_1k$. Como porém, $s_1 = a/d$, então $x = [(ab)/d]k$, o que mostra que $x \in \langle (ab)/d \rangle$ ■

**37.** Com base no item b do exercício anterior em $\mathbb{Z}[i]$, encontre um mínimo múltiplo comum dos elementos $\alpha$ e $\beta$ nos seguintes casos:

a) $\alpha = 3$ e $\beta = 7$;

b) $\alpha = 6$ e $\beta = 9 + 12i$.

## 4. POLINÔMIOS SOBRE ANÉIS FATORIAIS

Nesta seção o símbolo $A$ indicará sempre um anel fatorial infinito. Vale lembrar que, como mostramos em **3.2**, dois elementos quaisquer de um anel fatorial sempre têm máximo divisor comum. Esse resultado, obviamente, pode ser estendido para um número finito qualquer de elementos do anel.

**Definição 8:** Um polinômio não constante pertencente a $A[x]$ se diz *primitivo* se a unidade de $A$ é um máximo divisor comum de seus coeficientes. Em outras palavras, isso significa que os únicos divisores dos coeficientes do polinômio são os elementos inversíveis do anel.

*Exemplo 13:* O polinômio $f(x) = 2 + 2x + 3x^2 \in \mathbb{Z}[x]$ é primitivo, pois $\mathrm{mdc}(2, 3) = 1$.

**Proposição 9:** Seja $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in A[x]$ um polinômio não nulo. Então existem um elemento $d \in A$ e um polinômio primitivo $f^* \in A[x]$, de mesmo grau que $f$, tais que $f = df^*$.

*Demonstração:* Se $d = \text{mdc}(a_0, a_1, ..., a_n)$, então $a_0 = dq_0, a_1 = dq_1, ..., a_n = dq_n$, para convenientes elementos $q_0, q_1, ..., q_n \in A$, primos entre si. Daí:

$$f(x) = (dq_0) + (dq_1)x + (dq_2)x^2 + ... + (dq_n)x^n = d(q_0 + q_1x + q_2x^2 + ... + q_nx^n).$$

Fazendo-se $f^*(x) = q_0 + q_1x + q_2x^2 + ... + q_nx^n$, então $f^*$ tem o mesmo grau de $f$, é primitivo e $f = df^*$. #

**Proposição 10:** Seja $f \in A[x]$ um polinômio não constante. Se $f$ é irredutível, então $f$ é primitivo.

*Demonstração:* De fato, suponhamos que $f$ não fosse primitivo e indiquemos por $d$ um máximo divisor comum de seus coeficientes. Então, devido à proposição anterior, $f = df^*$, em que $\partial(f^*) = \partial(f)$. Observemos porém que, como $d$ não é inversível em $A$, também não o é em $A[x]$. Por outro lado, $f^*$ também não é inversível em $A[x]$, já que tem o mesmo grau de $f$ (lembrar que os inversíveis de $A[x]$ são os mesmos de $A$ e, portanto, têm grau zero). Então $f = df^*$ é uma decomposição não trivial de $f$ em $A[x]$, o que contraria a hipótese de $f$ ser irredutível sobre $A$. De onde, $f$ é primitivo. #

*Contra-exemplo 3:* Um polinômio primitivo pode não ser irredutível.

O polinômio $f(x) = 2 + 5x + 2x^2$ é primitivo, mas composto em $\mathbb{Z}[x]$, uma vez que

$$f(x) = (2x + 1)(x + 2)$$

Nosso objetivo agora é demonstrar o *critério de irredutibilidade de Eisenstein* para polinômios sobre um anel fatorial. Ferdinand R. Eisenstein (1823-1852), alemão, foi um brilhante matemático, muito admirado por Gauss, com quem estudou. Ao morrer precocemente, aos 29 anos de idade, Eisenstein já era professor da Universidade de Berlim e membro da Academia de Ciências dessa cidade, graças a uma produção científica volumosa e especialmente brilhante.

Para chegar ao critério de Eisenstein precisaremos de três lemas.

**Lema 3:** Se $f, g \in A[x]$ são polinômios primitivos e para elementos $a, b \in A$ vale a igualdade $af = bg$, então $a \sim b$ e $f \sim g$.

*Demonstração:* Façamos $af = h$ e seja $d$ um máximo divisor comum dos coeficientes de $h$. Então $h = dh^*$, em que $h^*$ é um polinômio primitivo e de mesmo grau que $h$ (proposição 9). Por outro lado, como $af = h$, então $a$ divide todos os coeficientes de $h$ e, portanto, $a \mid d$ em $A$. Logo, $d = ac$, para um conveniente elemento $c \in A$. Desse modo:

$$h = dh^* = ach^* = af$$

e o cancelamento de $a$ na última igualdade leva a $f = ch^*$, o que mostra que $c$ divide $f$ e, portanto, seus coeficientes, já que $c \in A$. Como $f$ é primitivo, então $c$ é inversível. Levando-se em conta que $d = ac$, conclui-se que $d \sim a$. Da mesma forma demonstra-se que $d \sim b$. De onde, $a \sim b$.

Agora, o fato de $a$ e $b$ serem associados implica a existência de um elemento inversível $u \in A$ tal que $b = au$. Usando esse fato em $af = bg$ (hipótese), obtemos $af = aug$ e, portanto, $f = ug$, em que $u$ é inversível em $A$ e, portanto, em $A[x]$. Isso mostra que $f \sim g$, como queríamos demonstrar. #

**Lema 4** (lema de Gauss): O produto de dois polinômio primitivos $f, g \in A[x]$ também é um polinômio primitivo.

*Demonstração:* Suponhamos $f$ e $g$ definidos respectivamente por $f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ e $g(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s$ e que o produto $fg = c_0 + c_1x + c_2x^2 + ... + c_{r+s}x^{r+s}$ não fosse primitivo. Existiria então em $A$ um elemento irredutível $p$ divisor de todos os coeficientes de $fg$. Mas esse elemento não divide todos os coeficientes de $f$, nem tampouco todos os de $g$. Seja $a_m$ o coeficiente de $f$ não divisível por $p$ com maior índice e, analogamente, $b_n$ o coeficiente de $g$ não divisível por $p$ com maior índice. Observemos então o coeficiente

$$c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + ... + a_mb_n + ... + a_{m+n-1}b_1 + a_{m+n}b_0$$

Devido às suposições feitas, $p$ divide todas as parcelas do segundo membro dessa igualdade anteriores e posteriores ao produto $a_mb_n$. Como $p \mid c_{m+n}$, então $p \mid a_mb_n$ e, sendo irredutível, divide um desses fatores. Como essa conclusão é contraditória com a escolha dos coeficientes $a_m$ e $b_n$, então a suposição de que $fg$ não é primitivo deve ser descartada. De onde, a tese. #

**Lema 5:** Seja $K$ o corpo das frações de $A$. Se o polinômio $f \in A[x]$ é irredutível sobre $A$, então também é irredutível sobre $K$.

*Demonstração:* Suponhamos, por absurdo, que $f$ fosse composto em $K[x]$. Existiriam então polinômios $g, h \in K[x]$, de grau $\geqslant 1$, tais que $f = gh$. Os coeficientes de $f$ e $g$ são frações cujos termos pertencem a $A$. Indicando-se por $a$ o produto dos denominadores dessas frações:

$$af = g_1h_1 \qquad (2)$$

em que $g_1$ e $h_1 \in A[x]$ e têm o mesmo grau que $g$ e $h$, respectivamente. Se $b$, $c$ e $d$ denotam, respectivamente, máximos divisores comuns dos coeficientes de $f$, $g_1$ e $h_1$, então:

$$f = bf_1, \; g_1 = cg_2 \quad \text{e} \quad h_1 = dh_2 \qquad (3)$$

em que $f_1$, $g_2$ e $h_2$ são primitivos e de mesmo grau que $f$, $g_1$ e $h_1$, respectivamente (proposição 9). De (2) e (3) resulta:

$$abf_1 = cdg_2h_2$$

Como $g_2h_2$ é primitivo, devido ao lema de Gauss, então o lema 3 garante que $ab \sim cd$ e $f_1 \sim g_2h_2$. Assim:

$$f_1 = ug_2h_2$$

para um conveniente elemento inversível $u \in A$, e, portanto:

$$f = bf_1 = (ubg_2)h_2$$

Como $(ub)g_2$ e $h_2$ são polinômios de $A[x]$ que têm graus iguais aos de $g_1$ e $h_1$, respectivamente, e, portanto, $\geqslant 1$, então $f$ é composto sobre $A$, o que é absurdo, uma vez que essa conclusão contraria a hipótese. #

**Proposição 11** (critério de Eisenstein): Seja $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in A[x]$. Se existir um elemento irredutível $p \in A$ que seja divisor de $a_0, a_1, ..., a_{n-1}$ mas não de $a_n$ e se $p^2$ não divide $a_0$, então $f$ é irredutível sobre o corpo das frações de $A$.

*Demonstração:* Seja $K$ o corpo das frações de $A$ e suponhamos $f$ composto em $K[x]$. Então $f$ é o produto de dois polinômios de grau $\geqslant 1$ de $K[x]$. Mas, considerada a contrapositiva do lema anterior, $f$ também poderia ser decomposto em um produto de dois fatores não triviais de $A[x]$:

$$f(x) = (b_0 + b_1x + b_2x^2 + ... + b_rx^r)(c_0 + c_1x + c_2x^2 + ... + c_tx^t)$$

Como $p \mid a_0 = b_0c_0$ e $p^2$ não divide $a_0$, então $p \mid b_0$ ou $p \mid c_0$, exclusivamente. Suponhamos que $p \mid b_0$. Como $p$ não divide $a_n = b_rc_t$, então $p$ não divide $b_r$. Isso posto, seja $s$ $(0 < s \leqslant r < n)$ o menor índice tal que $p$ não divide $b_s$. Portanto, $p \mid b_0$, $p \mid b_1, ..., p \mid b_{s-1}$ e p não divide $b_s$.

Como

$$a_s = b_0c_s + b_1c_{s-1} + b_2c_{s-2} + ... + b_{s-1}c_1 + b_sc_0$$

e $p \mid a_s$, pois $s < n$, então $p \mid b_sc_0$. Não dividindo $c_0$, então $p \mid b_s$, o que é absurdo. #

*Exemplo 14:* O polinômio $f(x) = 7 + 14x + x^{60} \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$. De fato, considerando o número primo $p = 7$, vemos que $7 \mid 7$, $7 \mid 14$, 7 não divide 1 e $7^2$ não divide 7. Uma generalização simples do exemplo dado mostra que em $\mathbb{Q}[x]$ existem polinômios irredutíveis de grau arbitrariamente grandes.

Para encerrar o capítulo, mostraremos que, se um anel $A$ é fatorial, então $A[x]$ também o é, mas que $A$ pode ser principal sem que $A[x]$ o seja.

Usaremos para isso o seguinte fato: se $a \in A$ é irredutível como elemento desse anel, então também é irredutível como elemento de $A[x]$. Vejamos a justificação. Primeiro, $a$ não é nulo (pois $A$ e $A[x]$ têm o mesmo zero) e não é inversível em $A[x]$, pois os inversíveis desse anel são os mesmos de $A$. Por outro lado, uma decomposição de $a$ em um produto de dois fatores de $A[x]$ só é possível se esses fatores tiverem grau zero e, portanto, pertencerem a $A$. Logo, é uma decomposição em $A$, e, devido à hipótese, um dos fatores é inversível em $A$. Portanto, esse fator também é inversível em $A[x]$.

É necessário também o lema seguinte.

**Lema 6:** Seja $A$ um anel fatorial. Então todo polinômio irredutível $f \in A[x]$ também é primo.

*Demonstração:* Suponhamos que $f \mid gh$ em $A[x]$. Denotando-se por $K$ o corpo das frações de $A$, é claro que $f$ também divide $gh$ em $K[x]$. Mas, como $f$ é irredutível sobre $K$ (lema 5) e $K[x]$ é principal, então $f$ é primo em $K[x]$ e, portanto, $f \mid g$ ou $f \mid h$ (novamente em $K[x]$). Trabalhemos com a primeira dessas possibilidades.

Existe então um polinômio $m' \in K[x]$ tal que $g = m'f$. Mas, se $c$ é o produto dos denominadores de $m'$, então $cm' = m$, ou $\frac{1}{c}m = m'$, em que $m \in A[x]$ e tem o mesmo grau que $m'$. Consideremos agora a decomposição fornecida pela proposição 9 para $g$ e $m$: $g = ag^*$ e $m = dm^*$, em que $a, d \in A$ e $g^*, m^* \in A[x]$, são primitivos e têm o mesmo grau que $g$ e $m$, respectivamente. Logo:

$$ag^* = g = m'f = \left(\frac{1}{c}m\right)f = \left(\frac{1}{c}dm^*\right)f$$

Daí:

$$acg^* = dfm^*$$

Mas $fm^*$ também é primitivo e, portanto, devido ao lema 3:

$$ac \sim d \quad \text{e} \quad g^* \sim fm^*$$

Logo:

$$g^* = ufm^*$$

para algum elemento inversível $u \in A$, e daí:

$$g = aufm^*$$

igualdade que mostra que $f \mid g$ em $A[x]$. #

**Proposição 12:** Se um anel $A$ é fatorial, então $A[x]$ também é um anel fatorial.

*Demonstração:* Seja $f \in A[x]$, $f \neq 0$ e $f$ não inversível.

(i) (Decomposição em fatores irredutíveis)

Raciocinaremos por indução sobre o grau de $f$. Se $\partial(f) = 0$, entao $f \in A$. Decompondo $f$ em fatores irredutíveis de $A$ (o que é possível, pois $A$ é fatorial), teremos a decomposição desejada, uma vez que, como vimos, esses fatores também são irredutíveis em $A[x]$.

Suponhamos agora que $\partial(f) = n > 0$ e tomemos por hipótese que a decomposição seja possível para todo polinômio de grau $r$, com $0 \leqslant r < n$. Devido à proposição 9, se $d$ é o máximo divisor comum dos coeficientes de $f$, então existe um polinômio primitivo $f^* \in A[x]$ tal que $f = df^*$. Caso $f^*$ seja irredutível, basta decompor $d$ em fatores irredutíveis para obter a decomposição desejada para $f$. (Neste caso, se $d$ fosse inversível, $f = df^*$ seria essa decomposição.) Caso $f^*$ seja composto, então existem polinômios $g, h \in A[x]$ tais que

$$1 \leqslant \partial(g),\ \partial(h) < \partial(f^*) \quad \text{e} \quad f^* = gh$$

Aplicando a hipótese de indução para $g$ e $h$ e raciocinando com $d$ como no caso anterior, obteremos a decomposição de $f$ conforme o enunciado

(ii) (Unicidade)

A demonstração fica como exercício. Sugerimos ler a demonstração da proposição 7 e frisamos que o lema anterior é imprescindível para o raciocínio $\#$

*Exemplo 15:* Como $\mathbb{Z}$ é fatorial, o mesmo se pode dizer de $\mathbb{Z}[x]$.

*Contra-exemplo 4:* Mostraremos agora que o anel fatorial $\mathbb{Z}[x]$ não é principal, embora $\mathbb{Z}$ o seja. Com isso, mostraremos também que não vale a recíproca da proposição 7. Para isso basta dar um exemplo de um ideal em $\mathbb{Z}[x]$ que não seja principal. É o caso de $I = \langle 2, x \rangle$. De fato, se $I$ fosse principal, existiria um polinômio $f \in \mathbb{Z}[x]$ tal que $I = \langle f \rangle$. Então, por pertencerem a $I$, os polinômios 2 e $x$ poderiam ser escritos na forma $2 = fg$ e $x = fh$, para convenientes polinômios $g, h \in \mathbb{Z}[x]$. Daí, $f \mid 2$ em $\mathbb{Z}[x]$ e, portanto, $f = \pm 1$ ou $f = \pm 2$. Mas como, também, $f \mid x$ e nem $+2$ nem $-2$ são divisores de $x$ em $\mathbb{Z}[x]$, segue que $f = \pm 1$. Então $I = \mathbb{Z}[x]$ e, portanto, todo polinômio de $\mathbb{Z}[x]$ seria do tipo

$$2(a_0 + a_1x + a_2x^2 + \ldots + a_rx^r) + x(b_0 + b_1x + b_2x^2 + \ldots + b_sx^s) =$$
$$= 2a_0 + (2a_1 + b_1)x + (2a_2 + b_2)x + \ldots$$

ou seja, teria como primeiro coeficiente, escrito na forma padrão, um número par, o que é absurdo. Logo, efetivamente o ideal $I \quad \langle 2, x \rangle$ não é principal e, por consequência, $\mathbb{Z}[x]$ não é um anel principal.

## Exercícios

**38.** Considere os ideais $I \quad \langle x, 2x + 1 \rangle$ e $J = \langle x, 5x + 2 \rangle$ em $\mathbb{Z}[x]$. Mostre que $I$ é principal mas $J$ não é. Algum deles é maximal? Justifique.

**39.** Represente cada um dos polinômios de $A[x]$ na forma de um produto de um elemento de $A$ por um polinômio primitivo sobre $A$:

a) $3x^2 + 6x + 6, A = \mathbb{Z}$

b) $2x^2 + 2x + 1, A = \mathbb{R}$

c) $2x^2 + (1 + i)x + (1 - i), A = \mathbb{Z}[i]$

d) $2x^2 + \left(2 - \sqrt{2}\right)x + 4, A = \mathbb{Z}\left[\sqrt{2}\right]$

**40.** Seja $A$ um anel de integridade infinito. Se $K$ é o corpo das frações de $A$, represente cada um dos polinômios de $K[x]$ como o produto de um elemento de $K$ por um polinômio primitivo sobre $A$:

a) $\frac{1}{3}x^2 + \frac{1}{2}x + 6, A = \mathbb{Z}$

b) $\frac{1}{2}x^2 \quad \frac{5}{1 \quad i}x + 2, A = \mathbb{Z}[i]$

c) $\frac{1}{4}x^2 + \frac{1}{2}x + \frac{1}{4 \quad 2\sqrt{2}}, A = \mathbb{Z}\left[\sqrt{2}\right]$

**41.** Mostre, através do critério de Eisenstein, que são irredutíveis sobre $\mathbb{Q}$ os seguintes polinômios inteiros:

a) $2 + 2x + 4x^2 + x^3$

b) $x^{500} - 7$

**42.** Mostre, através do critério de Eisenstein, que são irredutíveis sobre o corpo das frações de $A$ os seguintes polinômios:

a) $x^4 - (2i)x^3 + (1 + i)x^2 + (1 - i)$, $A = \mathbb{Z}[i]$

b) $x^4 - 3$, $A = \mathbb{Z}[i]$

c) $x^3 - 3x^2 + 6x + 1 + \sqrt{-2}$, $A = \mathbb{Z}\left[\sqrt{-2}\,\right]$

**43.** A recíproca do lema 5 é verdadeira ou falsa? Prove ou contra-exemplifique.

**44.** Sejam $A$ um anel fatorial infinito e $p \in A$. Se $p$ é primo em $A$, prove que $p$ também é primo em $A[x]$.

**45.** Seja $A$ um anel fatorial infinito. Prove que um divisor de um polinômio primitivo $f \in A[x]$ também é primitivo.

**46.** Sejam $A$ um anel de integridade e $\varphi: A \to A$ um isomorfismo de anéis. Prove que:

a) se $p \in A$ é um elemento primo, então $\varphi(p)$ também é primo;

b) se $p \in A$ é um elemento irredutível, então $\varphi(p)$ também é irredutível.

**47.** Seja $A$ um anel de integridade infinito. Mostre que $\varphi: A[x] \to A[x]$ definida por $\varphi(f) = g$, em que $g(x) = f(x + 1)$, para todo $x \in A$, é um isomorfismo de anéis.

**48.** Se $p$ é um número primo, mostre que é irredutível sobre $\mathbb{Q}$ o polinômio inteiro $f$ definido por $f(x) = 1 + x + x^2 + \dots + x^{p-1}$.

*Sugestão:* Observar que $f(x) = \dfrac{x^{p} - 1}{x - 1}$, usar o isomorfismo introduzido no exercício 47 e, a seguir, o critério de Eisenstein.

# RESPOSTAS DE ALGUMAS QUESTÕES

**Capítulo I**

**1.** verdadeiras: a, c, d
falsas: b, e

**2.** $B = \{1\}$, $C = \{\varnothing, 1, \{1\}, \{1, 2\}\}$

**3.** a) $A = \{1, 2, 3, 4\}$, $B = \{4, 5\}$ e $C = \{3, 4, 5\}$
b) $A = \{1, 2, 3, 4, 5\}$, $B = \{4, 5, 6, 7\}$ e
$C = \{4, 5, 6, 7, 8\}$

**7.** a) $\mathcal{P}(A) = \{\varnothing, \{\varnothing\}, \{1\}, \{\{1\}\}, \{\varnothing, 1\}, \{\varnothing, \{1\}\},$
$\{1, \{1\}\}, \{\varnothing, 1, \{1\}\}\}$
c) 64

**9.** 470

**11.** a) $\varnothing$
b) $I$ (conjunto dos números irracionais)
c) $\varnothing$
d) $\{1/2, 3/4, 5/6, ...\} = \left\{\frac{2n-1}{2n}; n = 1, 2, 3, ...\right\}$
e) $A$

**12.** 4

**13.** a) respectivamente: $I, I, [5, +\infty[$, $\{1/2, 3/4, 5/6, ...\}$, $A \cup B$

**16.** $A = \{2, 4, 6, 8, 10\}$
$B = \{3, 6, 9, 12\}$
$C = \{4, 8, 12\}$

**17.** verdadeiras: a, b, c, d, f, g, i
falsas: e, h, j

**18.** a, b, d, e

**19.** a) Se $\Delta$ é um triângulo, então qualquer lado de $\Delta$ é menor que a soma dos outros dois
b) Se $p$ é um número primo diferente de 2, então $p$ é ímpar
c) Se $x$ é um número real tal que $-2 < x < 2$, então $x^2 < 4$.
d) Se duas retas são paralelas entre si e se não são paralelas ao eixo das ordenadas, então essas retas têm o mesmo coeficiente angular.
e) Se uma função real de variável real é diferenciável num ponto, então ela é contínua nesse ponto.
f) Se uma das filas de um determinante é formada de zeros, então esse determinante é nulo.

**20.** verdadeiras: b, c
falsas: a, d

**21.** a) Existe $x$, $x > 2$, tal que $x^2 < 4$.
b) Existe um triângulo retângulo que é eqüilátero.
c) Existe um número real $x$ tal que, qualquer que seja o inteiro $n$, verifica-se $n \leqslant x$.
d) Qualquer que seja o número complexo $z$, vale $z^5 \neq -2$.
e) Existem retângulos que não são paralelogramos.
f) Existem planos paralelos tais que um deles contém uma reta que não é paralela ao outro.

**22.** a) $\exists x$ b) $\forall x$ c) $\forall x$ d) $\exists x$ e) $\exists x$ f) $\exists x$

**23.** a) $(\forall x)(\exists y)$ b) $(\forall x)(\forall y)$ c) $(\exists x)(\exists y)$ d) $(\exists x)(\exists y)$ e) $(\forall x)(\forall y)$

**24.** verdadeiras: a, c
falsas: b

**25.** a, c, d

**26.** b, d, e

**27.** Recíprocas:

a) Se a soma de dois números inteiros é par, então esses números são ímpares.

b) Se uma função real de variável real é diferenciável num ponto, então ela é contínua nesse ponto.

c) Se o determinante de uma matriz é diferente de zero, então a matriz correspondente é inversível.

d) Se um polinômio real tem duas e apenas duas raízes complexas, então esse polinômio tem grau 2.

e) Se todas as retas de um plano são perpendiculares a um outro plano, então os dois planos são perpendiculares entre si.

Contrapositivas:

a) Se a soma de dois números inteiros é ímpar, então um deles é par.

b) Se uma função real de variável real não é diferenciável num ponto, então ela não é contínua nesse ponto.

c) Se o determinante de uma matriz é igual a zero, então essa matriz não é inversível.

d) Se o número de raízes complexas de um polinômio real é diferente de dois, então o grau desse polinômio é diferente de 2.

e) Se num plano há uma reta que não é perpendicular a um segundo plano, então os dois planos não são perpendiculares.

**28.** Recíprocas:
verdadeiras: b, c, d, e
falsas: a
Contrapositivas:
verdadeiras: a, c, d
falsas: b, e

**29.** Se $a < c$, então $a \leq b$ ou $b < c$.

**30.** Se três pontos distintos, $A$, $B$ e $C$, de um plano são tais que $AB \geq AC + BC$, então esses pontos são colineares.

**31.** a) $x - 1$ c) $x - 0$
b) $x \quad 10$ d) $x - 1/2$

**Capítulo II**

**10.** a = 57, 56, 55, 54 e, respectivamente, r = 4, 18, 32, 46

**12.** 111

**16.** c) mdc (42, −96) = 6
$42 \cdot 7 + (-96) \cdot 3 = 6$

**17.** 48

**18.** 500 e 180

**24.** $780 = 2^2 \cdot 3 \cdot 5 \cdot 13$

**25.** b) $2^2 \cdot 3^1 \cdot 5^0 \cdot 13^0 \cdot 13^0 = 12$

**31.** 144

**33.** b) $\{(2 - 2t, 4 - 5t) \mid t \in \mathbb{Z}\}$
d) $\{(18 + 23t, \; 3 - 4t) \mid t \in \mathbb{Z}\}$

**34.** 56 e 44

**35.** $-60 - 77t$ ($t = -1, -2, -3, \ldots$)

**36.** 60 inteiras e 4 meias

**37.** $-255 - 37t$ ($t = -7, -8, -9, \ldots$)

**38.** a) 1 b) 1 d) 0

**40.** 0

**45.** a) $x \equiv 1103 \pmod{2210}$
b) $x \equiv 4128 \pmod{6061}$

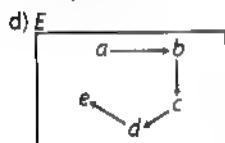
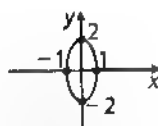
**46.** a) $x \equiv 851 \pmod{1430}$
b) $x \equiv 26 \pmod{630}$

**47.** 3930

**Capítulo III**

**1.** a) $R_1 = \{(1, 0), (3, 2), (5, 4), (7, 6)\}$
$R_2 = \{(1, 2), (1, 4), (1, 6), (3, 4), (3, 6), (5, 6)\}$
$R_3 = \varnothing$

b) $D(R_1) = \{1, 3, 5, 7\}$ e $Im(R_1) = \{0, 2, 4, 6\}$
$D(R_2) = \{1, 3, 5\}$ e $Im(R_2) = \{2, 4, 6\}$
$D(R_3) = \varnothing$ $Im(R_3)$

**2.** a) $E = \{a, b, c, d, e\}$
b) $D(R) = \{a, b, c, d\}$ e $Im(R) = \{b, c, d, e\}$
c) $R^{-1} = \{(b, a), (c, b), (d, c), (e, d)\}$
$D(R^{-1}) = \{b, c, d, e\}$ e $Im(R^{-1}) = \{a, b, c, d\}$
d) $E$

**3.** a)

b) $D(R) = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$
c) $Im(R) = \{y \in \mathbb{R} \mid -2 \leq y \leq 2\}$
d) $R^{-1} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + 4y^2 = 4\}$

**4.** a) $R = \{(1, 3), (4, 2), (7, 1)\}$
b) $D(R) = \{1, 4, 7\}$
c) $Im(R) = \{1, 2, 3\}$
d) $R^{-1} = \{(3, 1), (2, 4), (1, 7)\}$

**5.** a) $mn$ b) $2^{mn}$

**6.** $R \cap R' = \varnothing$ e $R \cup R' = E \times E$

**7.** $R_1 \cup R_2 = \{(x, y) \mid xR_1y$ ou $xR_2y\}$
$R_1 \cap R_2 = \{(x, y) \mid xR_1y$ e $xR_2y\}$
$(x, y) \in R_1 \Rightarrow (x, y) \in R_2$

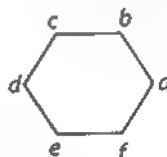
**8.** a) $R = \{(1, 1), (1, 3), (1, 5), (2, 2), (2, 4), (3, 1), (3, 3), (3, 5), (4, 4), (4, 2), (5, 5), (5, 3), (5, 1)\}$
b) $E$

c) $R$ é reflexiva, simétrica e transitiva; $R$ não é anti-simétrica.

**9.** $R$ é reflexiva, simétrica e transitiva.

**10.** $S$ não é reflexiva, simétrica, anti-simétrica e transitiva.

**11.** $R$ é simétrica (apenas).

**12.** a) 6
b) $R = \{(ab, ab), (ab, de), (de, ab), (de, de), (bc, bc), (bc, ef), (ef, bc), (ef, ef), (cd, cd), (cd, fa), (fa, cd), (fa, fa)\}$

c) reflexiva
simétrica
transitiva

**13.** reflexivas: $R_1$, $R_2$ e $R_4$
simétricas: $R_1$, $R_3$, $R_4$ e $R_5$
transitivas: $R_1$, $R_2$, $R_4$ e $R_5$
anti-simétricas: $R_1$, $R_2$ e $R_5$

**14.** $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3), (3, 2)\}$
$R_2 = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$
$R_3 = \{(1, 2), (2, 3), (1, 3), (2, 1)\}$
$R_4 = \{(1, 2), (2, 3), (3, 4)\}$

**16.** $\varnothing$, $\{(a, a)\}$, $\{(a, b)\}$, $\{(b, b)\}$, $\{(b, a)\}$, $\{(a, a), (a, b)\}$, $\{(a, a), (b, b)\}$, $\{(a, a), (b, a)\}$, $\{(a, b), (b, b)\}$, $\{(a, b), (b, a)\}$, $\{(b, b), (b, a)\}$, $\{(a, a), (a, b), (b, b)\}$, $\{(a, a), (b, b), (b, a)\}$, $\{(a, a), (a, b), (b, a)\}$, $\{(a, b), (b, b), (b, a)\}$, $E \times E$

**18.** reflexiva: $R_4$
simétricas: todas

**20.** reflexiva: $R_9$
simétricas: $R_7$ e $R_9$

**21.** $R_1$ e $R_4$

**22.** a

**24.** a

**27.** b) $\bar{0} = \{0, -2\}$, $\overline{-2} = \{0, -2\}$, $\bar{4} = \{4, -6\}$

**28.** b) $E/R = \{\{-3, -2, -1, 0\}, \{1\}, \{2\}, \{3\}\}$

**29.** a) $\bar{0} = \{0, 4, 8\}$, $\bar{1} = \{1, 5, 9\}$

b) $E/R = \{\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6, 10\}, \{3, 7\}\}$

**30.** b) $\overline{100} = \mathbb{Z}$

c) $\overline{0{,}5} = \left\{\frac{2x+1}{2} \mid x \in \mathbb{Z}\right\}$

**31.** b) classe do $\frac{1}{2} = \mathbb{Q}$

c) $\bar{a} = \mathbb{Q}, a \in \mathbb{Q}$

d) $\overline{\sqrt{2}} = \{x + \sqrt{2} \mid x \in \mathbb{Q}\}$

**32.** b) $\overline{1 + i} = \{(x, y) \in \mathbb{C} \mid x^2 + y^2 = 2\}$

**33.** $\mathbb{C}/R$ é o conjunto das retas paralelas ao eixo real.

**34.** $\overline{(0, 0)} = \{(x, y) \in \mathbb{R}^2 \mid xy = 0\}$

$\overline{(1, 1)} = \{(x, y) \in \mathbb{R}^2 \mid xy = 1\}$

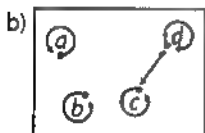
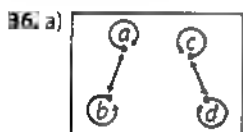
$\mathbb{R}^2/S$ é o conjunto de hipérboles $xy = k$.

**35.** $\overline{(1, 1)} = \{(x, y) \in \mathbb{R}^2 \mid x - y = 0\}$

$\overline{(1, 3)} = \{(x, y) \in \mathbb{R}^2 \mid x - y = -2\}$

$\mathbb{R}^2/T$ é o conjunto das retas paralelas à reta $x - y = 0$

**36.** a) a, b, c, d

b) a, d, b, c

c) congruência módulo 2

**37.** $R_1 = \{(a, a), (b, b)\}$ e $R_2 = E \times E$

**38.** $R_1 = \{(a, a), (b, b), (c, c)\}$

$R_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$

$R_3 = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$

$R_4 = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$

$R_5 = E \times E$

**39.** 15

**44.** a) 20, 10, 5, 4, 2, 1

b) 20, 10, 4, 5, 2, 1

**45.** $\{a, b\}$, $\{a\}$, $\{b\}$, $\varnothing$

**46.** 30, 6, 10, 15, 2, 3, 5

**47.** $\{a, b, c, d, e\}$, $\{a, b, c, d\}$, $\{a, b, c\}$, $\{a, b, d\}$, $\{a\}$, $\{b\}$

**48.** $\ell$. s. = $f, h, i$

$\ell$. i. = $b$

inf = $b$

sup = $f$

∄max

∄min

**49.** $\ell$. s. = $L \in \mathbb{Q} \mid L > \sqrt{2}$

$\ell$. i. = $\ell \in \mathbb{Q} \mid \ell < -\sqrt{2}$

∄ inf, sup, max, min

**50.** $\ell$. s. = 30

$\ell$. i. = 2

sup = 30

inf = 2

∄max

∄min

**51.** $\ell$. s. = $\{a, b, c, d\}$ e $\{a, b, c, d, e\}$

$\ell$. i. = $\{a\}$ e $\{b\}$

sup = $\{a, b, c, d\}$

∄inf

max = $\{a, b, c, d\}$

∄min

**52.** $\ell$. s. = $(x, y) \mid 2 \mid x$ e $2 \leq y$

$\ell$. i. = (1, 1) e (1, 0)

inf = (1, 1)

sup = (2, 2)

∄max

∄min

**53.** $R_2$ e $R_4$

**55.** $n \neq 0$

**56.** $f_1 = \{(0, 3), (1, 3), (2, 3)\}$
$f_2 = \{(0, 3), (1, 3), (2, 4)\}$
$f_3 = \{(0, 3), (1, 4), (2, 3)\}$
$f_4 = \{(0, 3), (1, 4), (2, 4)\}$
$f_5 = \{(0, 4), (1, 3), (2, 3)\}$
$f_6 = \{(0, 4), (1, 3), (2, 4)\}$
$f_7 = \{(0, 4), (1, 4), (2, 3)\}$
$f_8 = \{(0, 4), (1, 4), (2, 4)\}$

**57.** $f = \{(0, 1), (1, 1), (\frac{1}{2}, 1), (\sqrt{2}, -1), (\pi, -1), (\frac{7}{3}, 1)\}$

**58.** 1, 4, 1, 5, 0, respectivamente

**59.** $f(0) = 2, f\left(\frac{5}{3}\right) = 5, f\left(-\frac{7}{2}\right) = -2, f(\sqrt{3}) = 3\sqrt{3}$ e $f\left(-\frac{2\pi}{5}\right) = 5 - \frac{4\pi}{5}$

**60.** só no 1º e 2º casos

**61.** {7, 8}, {7, 8}, {6, 8, 9}, {6, 7, 8, 9}, {0, 1, 3, 4} e {5} respectivamente

**62.** 1, 3, $\sqrt{2} - 1$, [0, 1], [0, 2], $\mathbb{R}_+$, [−3, 3], [−3, 3] e ∅ respectivamente

**63.** [0, 2], $\mathbb{R}_+$, $\mathbb{R}_+$, $\{-1, 1, -4, 2\sqrt[3]{2}\}$, $[-4, 2\sqrt[3]{2}]$, ∅ respectivamente

**64.** a) 0
b) 1
c) 81
d) {(2, 4), (4, 2), (16, 1)}
e) {(5, 4), (25, 2), (625, 1)}
f) $\{(1, y) \mid y \in \mathbb{N}\} \cup \{(x, 0) \mid x \in \mathbb{N}\}$
g) 1
h) $\{(p, 1)\}$
i) $\{(0, y) \mid y \in \mathbb{N}^*\}$

**65.** $f_1, f_2$

**66.** $f_2, f_4$

**67.** $f_1 = \{(a, 1), (b, 2)\}$ $f_4 = \{(a, 3), (b, 2)\}$
$f_2 = \{(a, 2), (b, 1)\}$ $f_5 = \{(a, 3), (b, 1)\}$
$f_3 = \{(a, 2), (b, 3)\}$ $f_6 = \{(a, 1), (b, 3)\}$

**68.** $f_1 = \{(a, 1), (b, 1), (c, 2)\}$
$f_2 = \{(a, 1), (b, 2), (c, 1)\}$
$f_3 = \{(a, 2), (b, 1), (c, 1)\}$
$f_4 = \{(a, 1), (b, 2), (c, 2)\}$
$f_5 = \{(a, 2), (b, 1), (c, 2)\}$
$f_6 = \{(a, 2), (b, 2), (c, 1)\}$

**69.** $f_1 = \{(a, a), (b, b), (c, c)\}$
$f_2 = \{(a, a), (b, c), (c, b)\}$
$f_3 = \{(a, b), (b, a), (c, c)\}$
$f_4 = \{(a, b), (b, c), (c, a)\}$
$f_5 = \{(a, c), (b, a), (c, b)\}$
$f_6 = \{(a, c), (b, b), (c, a)\}$

**70.** a) 1, 5 e 12
b) não
c) sim

**73.** Injetoras: *b, d, e*
sobrejetoras: *b, e*

**76.** $a \neq 0$ e $c \neq 0$

**79.** a) não
b) sim
c) $\{(x, y) \mid x = 0 \text{ ou } y = 0\}$
d) [0, 2]
e) $\mathbb{R}_+$

**81.** 1º) $f(x) = x + 1$
2º) $f(x) = \begin{cases} 2x, \text{ se } x \geq 0 \\ -2x - 1, \text{ se } x < 0 \end{cases}$
3º) $f(x) = 2^x$
4º) $f(x) = \frac{b - a}{2} \cdot x + \frac{a + b}{2}$

**82.** $f^{-1}(x) = \frac{x - b}{a}$

**83.** $f^{-1}(x) = \frac{b - dx}{a - cx}$

**84.** $f^{-1}(x, y) = (x - 3, 2 - y)$

**85.** $g \circ f = \{(1, 8), (2, 8), (3, 9)\}$
nem injetora nem sobrejetora

**86.** $g \circ f = f$, $f \circ g = g$, $g \circ h = \{(a, d), (b, c), (c, c), (d, a)\}$, $h \circ g = \{(a, b), (b, b), (c, d), (d, c)\}$, $h \circ f = h$, $h \circ h = \{(a, b), (b, b), (c, b), (d, d)\}$

**87.** $(f \circ g)(x) = x^2 + 1$
$(g \circ f)(x) = x^2 + 4x + 3$
$(f \circ h)(x) = 3x + 2$
$(g \circ g)(x) = x^4 - 2x^2$
$(g \circ h)(x) = 9x^2 - 1$
$(h \circ g)(x) = 3x^2 - 3$

**88.** $(f \circ g)(x) = x^6 + 3x^4 + 3x^2 + 2$
$(g \circ f)(x) = x^6 + 2x^3 + 2$
$(f \circ f)(x) = x^9 + 3x^6 + 3x^3 + 2$
$(g \circ g)(x) = x^4 + 2x^2 + 2$

**89.** $a = \sqrt[3]{3}$ e $n = 2$

**90.** $g(x) = 2x^2 - x - 2$

**91.** $(f \circ g)(x) = \begin{cases} 3x - 1, \text{ se } x \geqslant \frac{2}{3} \\ -3x + 3, \text{ se } x < \frac{2}{3} \end{cases}$

$(g \circ f)(x) = \begin{cases} 3x + 1, \text{ se } x \geqslant 0 \\ -3x + 1, \text{ se } x < 0 \end{cases}$

**92.** $(f \circ f)(x) = \begin{cases} x + 2, \text{ se } x \leqslant -1 \\ -2x - 1, \text{ se } -1 < x \leqslant 0 \\ -1 + 4x, \text{ se } 0 < x < \frac{1}{2} \\ 2 - 2x, \text{ se } x \geqslant \frac{1}{2} \end{cases}$

**93.** $(f \circ g)(x) = \begin{cases} 2(1 - x), \text{ se } x < 1 \\ 2(1 + x), \text{ se } x \geqslant 1 \end{cases}$

$(g \circ f)(x) = \begin{cases} 1 + x^2, \text{ se } x \leqslant -1 \\ 1 - x^2, \text{ se } -1 < x < 0 \\ 1 - 2x, \text{ se } 0 < x < \frac{1}{2} \\ 1 + 2x, \text{ se } x \geqslant \frac{1}{2} \end{cases}$

**94.** $(f \circ g)(x) = x$
$(g \circ f)(x) = x$
então $g = f^{-1}$

**95.** a) $(f \circ g)(x) = x^2 - x + 2$
$(f \circ f)(x) = x + 4$
$(g \circ g)(x) = x^4 - 2x^3 + x$
b) $h(x) = x - 2$

**98.** c, e

**101.** $g, i$

**102.** $f^{-1} = \{(0, 0), (1, 1), (4, 2), (9, 3), (16, 4), (25, 5)\}$

**103.** $f, i_{\mathbb{R}}$

**104.** $g: \mathbb{R} \to \mathbb{R}$ tal que $g(x) = 2^x$

**105.** associativas: c, d, f

**106.** associativas: a, b, c, d, e

**107.** $c = 0, a \in \{1, -1\}$ e $b \in \{0, 1\}$
ou
$c \neq 0$ e $a = b = 1$

**108.** comutativas: a, c, d, f, i, j

**109.** comutativas: a, b, c, d, e

**110.** $a = b$

**111.** têm neutro: c, d, f, i

**112.** têm neutro: b, c, d, e

**113.** $e = \begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix}$ com $\alpha \in \mathbb{R}$

**114.** a) $m^2 = m$ e $n^2 = n$
b) $m = n$
c) $m = n = 1$

**115.** ($a = b = 0$ e $c \neq 0$) ou ($a = b \neq 0$ e $c$ qualquer)

**116.** c) 0
d) $x \mid x \in \mathbb{R}$
f) 0
i) $x \mid x \geqslant \frac{1}{2}$

**117.** b) $\mathbb{Z} \times \mathbb{Z}$
c) $\{(x, y) \mid x = \pm 1 \text{ e } y \in \mathbb{Z}\}$
d) $\{(x, y) \mid x \in \mathbb{Z} \text{ e } y = \pm 1\}$
e) $\{(1, 0), (0, 1), (-1, 0), (0, -1)\}$

**118.** $U_*(\mathbb{Z}^3) = \{(x, y, z) \mid x, y, z \in \{-1, 1\}\}$

**119.** b) $\{(x, y) \mid x \in U_*(E) \text{ e } y \in U_\Delta(F)\}$

**120.** a) $\mathbb{R}$
b) $\varnothing$
c) $\mathbb{R}_+$
d) $\mathbb{R}$
e) $\mathbb{R}^*$
f) $\mathbb{R} - \{1\}$
g) $\mathbb{Z} - \{0, -2\}$
h) $\mathbb{Q} - \{0, -1\}$
i) $\mathbb{R}$
j) $\mathbb{R}$

**121.** a) $\varnothing$
b) $\mathbb{Z} \times \mathbb{Z}$
c) $\mathbb{Z}^* \times \mathbb{Z}^*$
d) $\mathbb{Z} \times \mathbb{Z}^*$
e) $\mathbb{Z}^* \times \mathbb{Z}^*$

**123.** $\mathbb{R}$ $\quad \left\{\frac{3}{7}, \frac{5}{7}\right\}$

**126.** não existe

**127.** a, b, f

**128.** b, c, f

**132.** a)

| | 1 | 2 | 3 | 6 |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 1 | 2 |
| 3 | 1 | 1 | 3 | 3 |
| 6 | 1 | 2 | 3 | 6 |

b)

| | 1 | 3 | 9 | 27 |
|---|---|---|---|---|
| 1 | 1 | 3 | 9 | 27 |
| 3 | 3 | 3 | 9 | 27 |
| 9 | 9 | 9 | 9 | 27 |
| 27 | 27 | 27 | 27 | 27 |

c)

| | 1 | $\sqrt{2}$ | 3/2 |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| $\sqrt{2}$ | 1 | $\sqrt{2}$ | 3/2 |
| 3/2 | 1 | 3/2 | 3/2 |

d)

| | $3\sqrt{2}$ | $\pi$ | 7/2 |
|---|---|---|---|
| $3\sqrt{2}$ | $3\sqrt{2}$ | $3\sqrt{2}$ | 7/2 |
| $\pi$ | $3\sqrt{2}$ | $\pi$ | 7/2 |
| 7/2 | 7/2 | 7/2 | 7/2 |

e)

| | 1 | $i$ | $-1$ | $-i$ |
|---|---|---|---|---|
| 1 | 1 | $i$ | $-1$ | $-i$ |
| $i$ | $i$ | $-1$ | $-i$ | 1 |
| $-1$ | $-1$ | $-i$ | 1 | $i$ |
| $-i$ | $-i$ | 1 | $i$ | $-1$ |

**133.** a)

| $\cup$ | $\varnothing$ | {a} | {b} | {a, b} |
|---|---|---|---|---|
| $\varnothing$ | $\varnothing$ | {a} | {b} | {a, b} |
| {a} | {a} | {a} | {a, b} | {a, b} |
| {b} | {b} | {a, b} | {b} | {a, b} |
| {a, b} | {a, b} | {a, b} | {a, b} | {a, b} |

b)

| $\cap$ | $\varnothing$ | {a} | {b} | {a, b} |
|---|---|---|---|---|
| $\varnothing$ | $\varnothing$ | $\varnothing$ | $\varnothing$ | $\varnothing$ |
| {a} | $\varnothing$ | {a} | $\varnothing$ | {a} |
| {b} | $\varnothing$ | $\varnothing$ | {b} | {b} |
| {a, b} | $\varnothing$ | {a} | {b} | {a, b} |

c)

| * | $\varnothing$ | {a | {b} | {a, b} |
|---|---|---|---|---|
| $\varnothing$ | $\varnothing$ | {a} | {b} | {a, b} |
| {a} | {a} | $\varnothing$ | {a, b} | {b} |
| {b} | {b} | {a, b} | $\varnothing$ | {a} |
| {a, b} | {a, b} | {b} | {a} | $\varnothing$ |

**134.** a)

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

b)

| $\Delta$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

**135.** a)

| $\oplus$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

b)

| $\odot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

**136.**

| $\cup$ | A | B | C | D | E |
|---|---|---|---|---|---|
| A | A | A | A | A | A |
| B | A | B | B | B | B |
| C | A | B | C | B | C |
| D | A | B | B | D | D |
| E | A | B | C | D | E |

**137.**

a)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $a$ | $a$ |

b)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ |

c)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $b$ | $a$ |

d)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $a$ | $a$ |

e)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $a$ |
| $b$ | $a$ | $a$ |

f)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $b$ |
| $b$ | $a$ | $a$ |

g)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $a$ |
| $b$ | $b$ | $a$ |

h)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $a$ |
| $b$ | $a$ | $b$ |

i)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $b$ | $a$ |

j)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $a$ | $b$ |

k)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $b$ | $b$ |

l)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $b$ |
| $b$ | $b$ | $a$ |

m)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $b$ |
| $b$ | $a$ | $b$ |

n)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $a$ |
| $b$ | $b$ | $b$ |

o)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $b$ | $b$ |

p)

| | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $b$ |
| $b$ | $b$ | $b$ |

**138.** a) 2 b) 2 c) 2 d) 2 e) 2

**139.**

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |
| $f_2$ | $f_3$ | $f_4$ | $f_1$ | $f_2$ |
| $f_3$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ |
| $f_4$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |

a) $f_4$
b) todos
c) $f_4, f_2, f_3$ e $f_1$

**140.**

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ |
| $f_3$ | $f_3$ | $f_4$ | $f_1$ | $f_2$ |
| $f_4$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |

**141.** $f_1 = \{(0, 0), (1, 1)\}$
$f_2 = \{(0, 0), (1, 0)\}$
$f_3 = \{(0, 1), (1, 1)\}$
$f_4 = \{(0, 1), (1, 0)\}$

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_2$ | $f_2$ | $f_2$ |
| $f_3$ | $f_3$ | $f_3$ | $f_3$ | $f_3$ |
| $f_4$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |

**142.**

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_3$ | $f_4$ | $f_1$ |
| $f_3$ | $f_3$ | $f_4$ | $f_1$ | $f_2$ |
| $f_4$ | $f_4$ | $f_1$ | $f_2$ | $f_3$ |

**143.**

| | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_5$ | $f_6$ | $f_3$ | $f_4$ |
| $f_3$ | $f_3$ | $f_4$ | $f_1$ | $f_2$ | $f_6$ | $f_5$ |
| $f_4$ | $f_4$ | $f_3$ | $f_6$ | $f_5$ | $f_1$ | $f_2$ |
| $f_5$ | $f_5$ | $f_6$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ |
| $f_6$ | $f_6$ | $f_5$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |

**144.** a) comutativas: todas
b) têm neutro: todas
c) elementos simetrizáveis:
$\{6\}, \{1\}, \{\sqrt{2}\}, \{\pi\}, \{1, i, -1, -i\}$
d) elementos regulares:
$\{6\}, \{1\}, \{\sqrt{2}\}, \{\pi\}, \{1, i, -1, -i\}$

**145.** 1) $d$ 2) $c$ 3) $c$ 4) $c$ 5) $d$

**146.**

| $\cap$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $B$ | $C$ | $D$ |
| $B$ | $B$ | $B$ | $C$ | $D$ |
| $C$ | $C$ | $C$ | $C$ | $D$ |
| $D$ | $D$ | $D$ | $D$ | $D$ |

a) $A$ b) $A$ c) $A$

**147.** comutativas: a, c
têm neutro: a, b, c
elementos simetrizáveis:
a) a, b, c, d
b) b
c) todos

**148.**

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $b$ | $a$ | $d$ | $c$ |
| $b$ | $a$ | $b$ | $c$ | $d$ |
| $c$ | $d$ | $c$ | $a$ | $b$ |
| $d$ | $c$ | $d$ | $b$ | $a$ |

**149.**

| $*$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $b$ | $a$ | $c$ | $e$ |
| $c$ | $c$ | $a$ | $e$ | $b$ |

**150.**

| * | *a* | *b* | *c* | *d* |
|---|---|---|---|---|
| *a* | *a* | *b* | *c* | *d* |
| *b* | *b* | *d* | *a* | *c* |
| *c* | *c* | *a* | *d* | *b* |
| *d* | *d* | *c* | *b* | *a* |

**151.**

| * | *a* | *b* | *c* | *d* | *e* |
|---|---|---|---|---|---|
| *a* | *a* | *a* | *a* | *a* | *a* |
| *b* | *a* | *e* | *d* | *c* | *b* |
| *c* | *a* | *d* | *e* | *b* | *c* |
| *d* | *a* | *c* | *b* | *e* | *d* |
| *e* | *a* | *b* | *c* | *d* | *e* |

**152.** {1, 2, 4}, {1, 2, 6}, {1, 2, 12}, {1, 3, 6}, {1, 3, 12},{1, 4, 12}, {1, 6, 12}, {2, 3, 6}, {2, 4, 12}, {2, 6, 12}, {3, 4, 12}, {3, 6, 12}, {4, 6, 12}

**153.** $X \subset Y$ ou $Y \subset X$

**154.**

| | *e* | *a* | *b* | *c* |
|---|---|---|---|---|
| *e* | *e* | *a* | *b* | *c* |
| *a* | *a* | *e* | *c* | *b* |
| *b* | *b* | *b* | *e* | *e* |
| *c* | *c* | *a* | *e* | *c* |

**155.** Em $\mathbb{R}_+$, $x * y = \sqrt{x^2 + y^2}$

**156.**

| | *e* | *a* | *b* | *c* |
|---|---|---|---|---|
| *e* | *e* | *a* | *b* | *c* |
| *a* | *a* | *b* | *e* | *e* |
| *b* | *b* | *c* | *e* | *a* |
| *c* | *c* | *b* | *a* | *e* |

**157.**

| | *e* | *a* | *b* | *c* |
|---|---|---|---|---|
| *e* | *e* | *a* | *b* | *c* |
| *a* | *a* | *b* | *e* | *e* |
| *b* | *b* | *e* | *c* | *e* |
| *c* | *c* | *e* | *e* | *a* |

## Capítulo IV

**1.** c, f

**7.** a) sim
b) não, pois $U \cdot (\mathbb{Z} \times \mathbb{Z}) = \{(1, -1), (1, 1), (-1, 1), (-1, -1)\}$

**14.**

| | *e* | *a* |
|---|---|---|
| *e* | *e* | *a* |
| *a* | *a* | *e* |

**15.**

| | *e* | *a* | *b* |
|---|---|---|---|
| *e* | *e* | *a* | *b* |
| *a* | *a* | *e* | *e* |
| *b* | *b* | *e* | *e* |

**17.**

| | *e* | *a* | *b* | *c* |
|---|---|---|---|---|
| *e* | *e* | *a* | *b* | *c* |
| *a* | *a* | *b* | *c* | *e* |
| *b* | *b* | *c* | *e* | *a* |
| *c* | *c* | *e* | *a* | *b* |

**18.** $F = F_2 \circ F_4 \circ F_3$

**19.**

| | *e* | *a* | *b* | *c* | *d* | *f* |
|---|---|---|---|---|---|---|
| *e* | *e* | *a* | *b* | *c* | *d* | *f* |
| *a* | *a* | *b* | *c* | *d* | *f* | *e* |
| *b* | *b* | *c* | *d* | *f* | *e* | *a* |
| *c* | *c* | *d* | *f* | *e* | *a* | *b* |
| *d* | *d* | *f* | *e* | *a* | *b* | *c* |
| *f* | *f* | *e* | *a* | *b* | *c* | *d* |

**20.** $x = c^{-1}b^{-1}a^{-1}c\,b^{-1}$

**21.** $x = bc^{-1}b^{-1}$

**22.** $x = ba^{-1}$

**28.** *A*

**29.** *A*

**30.** *A*

**31.** *A*

**32.** não

**35.** subgrupos: H1 e H2

**36.** a, c

**37.** $\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$ e $\mathbb{Z}_4$

**38.** b) subgrupos: $\{e, c\}$, $\{e, f\}$, $\{e, d\}$ e $\{e, a, b\}$

**39.** b) subgrupos: $\{e, c\}$ e $\{e, b, d\}$

**44.**

| ⊕ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

subgrupos {0}, {0, 3}, {0, 2, 4}, *G*

**48.** homomorfismos: a, b, d, e, f

**49.** injetores: a (se $k \neq 0$), c, d, f
sobrejetores: c, e, f

**50.** a) $\{0\}$, se $k \neq 0$, ou $\mathbb{Z}$, se $k = 0$
b) $\{1, -1\}$
d) $\{0\}$
e) $\{(0, y) \mid y \in \mathbb{Z}\}$
f) $\{0\}$

**51.** $N(f) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = y\}$

**52.** endomorfismos: a, b, c, d, g
núcleos: a) $\{1, -1\}$
b) $\{\cos\theta + i \operatorname{sen}\theta \mid \theta \in \mathbb{R}\}$
c) $\{1\}$
d) $\{1\}$
g) $\left\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}$

**57.** $N(f) = \{0\}$
$\operatorname{Im}(f) = \mathbb{R}_+^*$

**58.** Todas são homomorfismos.
núcleos: a) $\{(e_G, y) \mid y \in J\}$
b) $\{(x, e_J) \mid x \in G\}$
c) $\{e_G\}$
d) $\{(e_G, e_J)\}$
e) $\{e_J\}$

**59.**

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $a$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $a$ |

**60.**

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $c$ | $e$ | $b$ |
| $b$ | $b$ | $e$ | $c$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

$x = a^{-1}c^2b = beb = c$

**64.** a)

| | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $f$ | $e$ |
| $b$ | $b$ | $c$ | $d$ | $f$ | $e$ | $a$ |
| $c$ | $c$ | $d$ | $f$ | $e$ | $a$ | $b$ |
| $d$ | $d$ | $f$ | $e$ | $a$ | $b$ | $c$ |
| $f$ | $f$ | $e$ | $a$ | $b$ | $c$ | $d$ |

b) $a^2 = b$, $b^{-2} = (b^{-1})^2 = d^2$, $c^{-3} = (c^{-1})^3 = c^3$
c) $x = b^{-1}a^{-1}c^{-1} = dfc = e$

**67.** $f^{-1}: \mathbb{R}_+^* \to \mathbb{R}$ tal que $f^{-1}(x) = \log_a x$

**71.** $f_1 = \{(e, e), (a, a), (b, b), (c, c)\}$
$f_2 = \{(e, e), (a, b), (b, c), (c, b)\}$
$f_3 = \{(e, e), (a, b), (b, a), (c, c)\}$
$f_4 = \{(e, e), (a, b), (b, c), (c, a)\}$
$f_5 = \{(e, e), (a, c), (b, b), (c, a)\}$
$f_6 = \{(e, e), (a, c), (b, a), (c, b)\}$

**74.** $[1]_+ = \mathbb{Z}$
$[3]_+ = 3\mathbb{Z}$
$[3] = \{..., 3^{-2}, 3^{-1}, 1, 3, 3^2, ...\}$
$[i] = \{1, i, -1, -i\}$

**76.** cíclico: $\mathbb{Z}_4$
não cíclico: grupo de Klein

**82.** $[b] = \{e, b, d, g\}$
$o(d) = 2$
$G$ não é cíclico
$x = c$

**99.** $H$, $1 + H$ e $2 + H$

**100.** $4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$ e $3 + 4\mathbb{Z}$

**101.** $H$, $f_2 H$ e $f_3 H$ à esquerda, com
$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$H$, $H f_2$ e $H f_4$ com $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

**103.** É finito porque:
$(a, b) \sim (c, d) \Rightarrow a - b \in \mathbb{Z}$ e $b = d$ (mod 2)
Então:
$\mathbb{Z} \times \mathbb{Z} / \mathbb{Z} \times 2\mathbb{Z} = \{\overline{(0, 0)}, \overline{(0, 1)}\}$

**104.** Há infinitas classes do tipo $(n, \overline{0}) + H$, com $n \in \mathbb{Z}$ e $0 \in \mathbb{Z}_2$.

**106.** $\mathbb{Z} + (-1) = \mathbb{Z}$
$\mathbb{Z} + \frac{1}{2} = \left\{\frac{2n + 1}{2} \mid n \in \mathbb{Z}\right\}$

**131.** $H = \{\overline{0}, \overline{3}\}$
$G/H = \{H, \overline{1} + H, \overline{2} + H\}$

| + | $H$ | $\overline{1} + H$ | $\overline{2} + H$ |
|---|---|---|---|
| $H$ | $H$ | $\overline{1} + H$ | $\overline{2} + H$ |
| $1 + H$ | $\overline{1} + H$ | $2 + H$ | $H$ |
| $\overline{2} + H$ | $2 + H$ | $H$ | $1 + H$ |

$H \quad \{\bar{0}, \bar{2}, 4\}$

$G/H \quad \{H, 1 + H\}$

| + | $H$ | $1 + H$ |
|---|---|---|
| $H$ | $H$ | $\bar{1} + H$ |
| $\bar{1} + H$ | $\bar{1} + H$ | $H$ |

**132.**

$\mathbb{Z}_8/H$

| + | $H$ | $\bar{1} + H$ | $\bar{2} + H$ | $\bar{3} + H$ |
|---|---|---|---|---|
| $H$ | $H$ | $\bar{1} + H$ | $\bar{2} + H$ | $\bar{3} + H$ |
| $\bar{1} + H$ | $\bar{1} + H$ | $\bar{2} + H$ | $\bar{3} + H$ | $H$ |
| $\bar{2} + H$ | $\bar{2} + H$ | $\bar{3} + H$ | $H$ | $\bar{1} + H$ |
| $\bar{3} + H$ | $\bar{3} + H$ | $H$ | $\bar{1} + H$ | $\bar{2} + H$ |

$\mathbb{Z}/2\mathbb{Z}$

| + | $\mathbb{Z}$ | $1 + 2\mathbb{Z}$ |
|---|---|---|
| $\mathbb{Z}$ | $\mathbb{Z}$ | $1 + 2\mathbb{Z}$ |
| $1 + 2\mathbb{Z}$ | $1 + 2\mathbb{Z}$ | $\mathbb{Z}$ |

**135.** $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ e $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

**136.** a) (1 8) (3 6 4) (5 7) = (1 8) (3 4) (3 6) (5 7)

b) (1 3 4) (2 6) (5 8 7) − (1 4) (1 3) (2 6) (5 7) (5 8)

c) (1 3 4 7 8 6 5 2) − (1 2) (1 5) (1 6) (1 8) (1 7) (1 4) (1 3) (1 2)

**137.** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 5 & 4 & 3 & 6 & 9 & 7 & 8 & 10 \end{pmatrix}$ (1 2) (3 5) (7 9 8)

**138.** a) +1 b) +1 c) −1 d) −1

**139.** a) ímpar b) ímpar

**140.** a) (1 7 9 2 5 3 8) (4 6); ímpar; −1

b) (1 6) (2 5) (3 4); ímpar; −1

**141.** a) par b) ímpar c) par

## Capítulo V

**10.** $a = 1, b = c = -2, d = 6$; sim

**16.**

| + | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $b$ |
| $b$ | $b$ | $a$ |

| · | $a$ | $b$ |
|---|---|---|
| $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ |

**17.**

| + | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $a$ | $c$ |
| $c$ | $c$ | $b$ | $a$ |

| · | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | | |
| $c$ | $a$ | | |

**18.**

| + | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $a$ | $d$ | $c$ |
| $c$ | $c$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $c$ | $b$ | $a$ |

| · | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $c$ | $d$ |
| $c$ | $a$ | $c$ | $c$ | $a$ |
| $d$ | $a$ | $d$ | $a$ | $d$ |

**20.** a, c, d

**21.** São subanéis: a, c, d

**22.** $L_1, L_2, L_3$

**25.** $\{\bar{0}\}$, $\{\bar{0}, \bar{3}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$ e $\mathbb{Z}_6$

**26.** $x = 1$

**27.** $x = 6$

**28.** $x = y = 3$

**29.** $x \in \{3, 7, 11\}$ e $y = 5$

**31.** inversíveis

a) $\{1, -1\}$; b) $\{\mathbb{Q}^*\}$;

c) $\{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$,

d) $\mathbb{Z}_3^*$; e) $\{\bar{1}, \bar{3}\}$; f) $\{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \overline{11}, \overline{13}\}$;

g) $\{A \in M_2(\mathbb{R}) \mid \det A \neq 0\}$,

h) $\{(1, 1)\}$, $\{(1, 2)\}$

regulares

a) $\mathbb{Z}^*$; b) $\mathbb{Q}^*$; c) $\mathbb{Z}^* \times \mathbb{Z}^*$;

d) e) f) g) h) idem inversíveis

**32.** anéis de integridade $\mathbb{Z}, \mathbb{Q}$

corpos: $\mathbb{Q}$ e $\mathbb{Z}_3$

**33.** divisores de zero: 0, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16,18, 20, 21, 22

elementos regulares: 1, 5, 7, 11, 13, 17, 19, 23

elementos inversíveis: 1, 5, 7, 11, 13, 17, 19, 23

**34.** a) $\mathbb{Q} - \{1\}$

b) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = \pm 1\}$

**35.** divisores de zero: $(0, y), y \in \mathbb{Z}^*$

**36.** $\mathbb{Z}_2$

**37.** a) $\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}$

b) $(\bar{3}, \bar{2})$

**38.** $B, D, E$ e $F$

**44.** $N(\mathbb{Z}) = \{0\}$
$N(\mathbb{Z}_6) = \{0\}$
$N(\mathbb{Z}_8) = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$
$N(\mathbb{Z}_2 \times \mathbb{Z}_4) = \{(0, 0), (0, \overline{2})\}$
$N(\mathbb{R}^{\mathbb{R}}) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(x) = 0, \forall x\}$

**51.** divisores próprios de zero: $(x, 0)$ ou $(0, y)$ com $x \neq 0_A$ e $y \neq 0_B$
inversíveis: $(x, y)$, com $x \in U(A)$ e $y \in U(B)$

**53.** $A$

**54.** Nem sempre, só se $K = \{0, 1\}$

**56.** É verdadeiro. Uma família de subcorpos de $\mathbb{R}$ é formada pelos conjuntos da forma $\mathbb{Q}[\sqrt{p}]$, $p$ primo e inteiro, $\mathbb{Q}[\sqrt{p}] = \{x + y\sqrt{p} \mid x, y \in \mathbb{Q}\}$.

**59.** São homomorfismos: c, d, e, f, g.

**60.** núcleos: c) $\{0\}$
d) $\{(0, y) \mid y \in \mathbb{Z}\}$
e) $\{(0, 0)\}$
f) $\{x \in \mathbb{Z} \mid x \equiv 0 \pmod{n}\}$
g) $\{0\}$

**61.** homomorfismos: a, b, e
núcleos: a) $\{(x, 0) \mid x \in \mathbb{Z}\}$
b) $\{(x, 0) \mid x \in \mathbb{Z}\}$
e) $\{0\}$

**65.** $A = B = \mathbb{Z} \times \mathbb{Z}$ e $f(x, y) = (x, 0)$

**68.** $f^{-1}(x) = x + 1$

**76.** a) Há 9 possibilidades:
1) $m = n = p = q = 0$
2) $m = p = q = 0$ e $n = 1$
3) $n = p = q = 0$ e $m = 1$
4) $m = n = p = 0$ e $q = 1$
5) $m = n = q = 0$ e $p = 1$
6) $m = p = 0$ e $n = q = 1$
7) $m = q = 0$ e $n = p = 1$
8) $n = p = 0$ e $m = q = 1$
9) $n = q = 0$ e $m = p = 1$

b) $f$ é automorfismo nos casos 7 e 8.

**77.** $f_1(x) = 0$ e $f_2(x) = x$

**78.** $f_1(x) = 0$, $f_2(x) = \overline{x}$, $f_3(x) = \overline{3x}$ e $f_4(x) = \overline{4x}$

**79.** $f_1(x) = (0, 0)$, $f_2(x) = (x, 0)$, $f_3(x) = (0, x)$ e $f_4(x) = (x, x)$

**80.** $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que $f(x, y) = px$ ou $f(x, y) = py$ com $p \in \mathbb{Z}$.

**85.** a) 3 b) 0 c) 0 d) 0 e) 24 f) 0

**86.** 0

**87.** $\mathbb{Z}_m$

**91.** Não; porque $1 \cdot 1_A = 1_A \neq 0_A$.

**99.** São ideais: a, b, c, e, g, i, j.

**100.** É ideal à esquerda: d

**102.**

| | |
|---|---|
| a) $\{\overline{0}, \overline{2}, \overline{4}\}$ | e) $\mathbb{Z}_8$ |
| b) $5\mathbb{Z}$ | f) $4\mathbb{Z}$ |
| c) $\mathbb{Q}$ | g) $\mathbb{R}$ |
| d) $\mathbb{R}$ | h) $\mathbb{C}$ |

**103.** $\{\overline{0}\}$; $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$; $\{\overline{0}, \overline{4}\}$ e $\mathbb{Z}_8$

**105.** b) $J = \{\overline{0}, \overline{8}\}$

**107.** b) 5 e $-5$

**117.** $\langle\langle 4\rangle, 6\rangle = \langle 2\rangle$

**122.** $\langle x\rangle$ em $\mathbb{Z}[x]$

**130.** $\mathbb{R}/\{0\} = \mathbb{R}$
$\mathbb{R}/\mathbb{R} = \{0\}$

**133.** $A = \mathbb{Z}$, $I = 4\mathbb{Z}$ e $A/I = \mathbb{Z}_4$

**135.** a) $N(f) = 4\mathbb{Z}$
b) $\sigma: \mathbb{Z} \to \mathbb{Z}_4$ tal que $\sigma(x) = \overline{x}$, com $\overline{x} = x + 4\mathbb{Z}$

## Capítulo VI

**1.** $f(0) = 1$; $f(1) = 16$; $f(-1) = 0$

**2.** $(4 - 2 - 2 - 1)^{36} = 1$

**3.** $(f + g)(x) = 12 - x + 5x^2 + 5x^3$
$(g - h)(x) = 3 + 4x + x^2 + 5x^3 - x^4$
$(h - f)(x) = -5 - x - 4x^2 + x^4$

**4.** $(fg)(x) = 14 + 21x - 26x^2 + 3x^3 - 4x^4$
$(gh)(x) = 14x - 21x^2 + 9x^3 - 3x^4 + x^5$
$(hf)(x) = 4x - 15x^3 + 15x^4 - 4x^5$

**5.** $a = 1, b = -1, c = 4; f\left(\frac{1}{2}\right) = \frac{1}{2}$

**7.** São subanéis: $A$ e $B$.
São ideais: $A$ e $B$

**8.** $x^3 - 6x^2 + 11x - 6 = 0$

**9.** $f(6) = 0$

**10.** $a = -1; b = 6, c = 1$

**11.** $a = 1$ e $b = c = 0$

**12.** $a = 2; b = 1; a - b = 1$

**13.** $a = 8; b = -9; c = 3$

**15.** se $a = 1, \partial f = 1$
se $a = -\frac{3}{2}, \partial f = 2$
se $a \neq 1$ e $a \neq -\frac{3}{2}, \partial f = 3$

**16.** $\partial(fg) = 10; \partial(f^2 - g^2) = 7;$
$\partial(f^2 + g^2) \leqslant 10$

**17.** $\partial(f - g) = 4$
$\partial f^3 = 12$
$\partial g^2 = 6$
$\partial(f + g)^3 = 12$

**19.** $ad = bc$

**20.** a) $a = \frac{p^2}{q^2}$, com $p, q \in \mathbb{Z}$ e $q \neq 0$
b) $a \in \mathbb{R}_+$
c) $a$ qualquer

**22.** $P(x) = x^3 + 9x^2 - 34x + 24$
$P(-1) = 66$

**23.** a) $P(x) = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6} + d$
b) $S = \frac{n(n+1)(2n+1)}{6}$

**27.** $0 \leqslant p \leqslant n - 1$

**28.** $p = q = 1$

**31.** $a = \frac{1}{34}, b = \frac{93}{34}$

**32.** $p(x) = x^2 - 3x + 2$

**33.** $\begin{cases} \text{quociente} = x^2 + x + 1 \\ \text{resto} = 0 \end{cases}$

**34.** $|a + b + c + d| = 96$

**35.** cinco

**36.** $m = \frac{5}{2}$

**37.** quociente $= \frac{Q}{2}$
resto $= R$

**40.** $2x^3 + x^2 + 3x - 1$

**41.** $r = 1$

**42.** $a = \frac{3}{10}, q(x) = \frac{3}{10}x^2 - \frac{1}{10}x - \frac{12}{10}$

**44.** 2, −2, 3 e −3

**45.** $p = -\frac{10}{3}$ e $q = -\frac{14}{3}$

**46.** $r = 231$

**48.** $P(x) = x^3 + x^2 - 4x + 2$

**50.** $r = x + 3$

**51.** $\begin{cases} P(x) = \frac{5}{2}x^3 + 10x^2 + \frac{5}{2}x - 5 \\ a_3 = \frac{5}{2} \end{cases}$

**52.** a) $a = 1$
b) $q(x) = 2x^3 - 2x$
$r(x) = -x + 12$

**55.** a) $\begin{cases} q = x^3 - 3x^2 + 9x - 27 \\ r = 0 \end{cases}$

b) $\begin{cases} q = x^3 + 3x^2 + 9x + 27 \\ r = 162 \end{cases}$

c) $\begin{cases} q = x^4 + 2x^3 + 4x^2 + 8x + 16 \\ r = 64 \end{cases}$

d) $\begin{cases} q = x^4 - 2x^3 + 4x^2 - 8x + 16 \\ r = 64 \end{cases}$

e) $\begin{cases} q = x^5 + x^4 + x^3 + x^2 + x + 1 \\ r = 0 \end{cases}$

f) $\begin{cases} q = x^5 - x^4 + x^3 - x^2 + x - 1 \\ r = 2 \end{cases}$

g) $\begin{cases} q = x^4 + 3x^3 + 9x^2 + 27x + 81 \\ r = 486 \end{cases}$

h) $\begin{cases} q = x^4 - 3x^3 + 9x^2 \quad 27x + 81 \\ r = 0 \end{cases}$

**56.** $(x - a)(x^4 + ax^3 + a^2x^2 + a^3x + a^4)$

**57.** $R(x) = 0; Q(0) \quad 1$

**58.** $\forall n \in \mathbb{N}$

**59.** $Q(x) = 2x^3 - \frac{7}{2}x + \frac{37}{4}$

**60.** $r = 257$

**63.** $a = -1; b = 1$

**64.** $a = -3; b = 2$

**66.** $a = 2; b = 1; m = 3$

**68.** $r = \frac{x^2}{8} + x + \frac{3}{2}$

**71.** $k \cdot (x^4 - x^3 - 6x^2 + 14x - 12) = 0$, com $k \neq 0$

**72.** 3

**73.** $a = 2; b = -2$

**74.** $m \neq 2$

**78.** $1, -1, 2, -2, 4, -4$

**79.** $S = \left\{1, 3, \frac{1}{3}\right\}$

**80.** $S = \left\{-1, \frac{1}{5}, \frac{1}{3}\right\}$

**81.** $S = \left\{2, 3, \frac{12}{5}\right\}$

**83.** $S = \{1, -1, 2, -3\}$

**84.** $S = \left\{11, \quad 3, -6, \frac{1 + i\sqrt{3}}{2}, \frac{-1 + i\sqrt{3}}{2}\right\}$

**85.** $S = \left\{1, -1, 2, \frac{1}{2}, \frac{-3 + \sqrt{5}}{2}, \frac{-3 - \sqrt{5}}{2}\right\}$

**86.** $S = \{1, -1, -4\}$

**88.** $x^4 \quad 5x^3 + 7x^2 \quad x \quad 2 \cdot 0$

**89.** $S = \quad 1, \frac{1}{2}, 1 + \sqrt{2}, 1 \quad \sqrt{2}$

**91.** É maior ou igual a 5

**93.** $S = \{ \quad 1, 2 + 3i, 2 \quad 3i$

**94.** $m = -2, n = 0$

**95.** $S = \{1, i, -i\}$

**96.** $S = \{1 + 2i, 1 - 2i, 2\}$

**97.** $f(x) = x^3 - 2x^2 + 3x - 4$

**98.** $f = x^4 - 5x^2 + 6$

**99.** $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{3}{4}$

**100.** $E = \frac{7}{2}$

**101.** $a^2 + b^2 + c^2 + d^2 = 47$

**103.** $S = \{2, -1, 3\}$

**104.** $S = \{2, 3, 5\}$

**105.** $S = \{-6, 3, -2\}$

**106.** $S = \{-6, -4, 3\}$

**107.** $h = -1$ ou $h = \frac{1}{2}$

**108.** $m = -3$
ou $\frac{3}{2}(1 + i\sqrt{3})$ ou $\frac{3}{2}(1 - i\sqrt{3})$

**109.** $S = \left\{\frac{3}{2}, -1\right\}$

**110.** $p = 4; q = 3$

**111.** $p = -2; q = 0$
ou $p = -1; q = 1$

**112.** $P(x) = -(x - 1)(x - 5)(x + 2)$

**113.** a) Em $\mathbb{Q}[x]$, $f = (x^2 + 2)(x^2 - 2)$

b) Em $\mathbb{R}[x]$, $f = (x^2 + 2)(x + \sqrt{2})(x - \sqrt{2})$.

c) Em $\mathbb{C}[x]$, $f = (x + i\sqrt{2})(x - i\sqrt{2})(x + \sqrt{2})(x \quad \sqrt{2})$.

**116.** $1 + x^4 = (1 \quad \sqrt{2}x + x^2)(1 + \sqrt{2}x + x^2)$

**119.** a, b, d

**120.** a) Em $\mathbb{Z}[x]$, $f = 4(1 + 2x^2)$ é redutível.

b) Em $\mathbb{R}[x]$, $f$ é irredutível, pois 4 é inversível

c) Em $\mathbb{C}[x]$, $f = 4(-i + \sqrt{2}x)(+i + \sqrt{2}x)$ é redutível.

**121.** $a = 6$ ou $a = 10$

## Capítulo VII

**6.** b) $\mathbb{Z}/\sim\ = \{\{0\}, \{-1, 1\}, \{-2, 2\}, ...\}$

**9.** a) (i): verdadeira

(iii): falsa;

**10.** divisores de $1 + 2i$: $\pm 1, \pm i, 1 + 2i, -1 - 2i, -2 + i, 2 - i$

**16.** a) $\{-1, 1\}$

**18.** a) $\{-1, 1\}$

**19.** a) $\{-1, 1\}$

**20.** divisores comuns: $\pm 1, \pm 3, 2 + \sqrt{5}, 2 - \sqrt{5}$

**30.** a) quociente $= 1$, resto $= -1 - 3i$

**32.** b) quociente $= -3 + 2\sqrt{2}$;

resto $= 2 + \sqrt{2}$

**35.** Um máximo divisor comum é 3.

**37.** b) $-18 + 24i$

**39.** a) $3(x^2 + 2x + 2)$

b) $2x^2 + 2x + 1$ é primitivo em $\mathbb{R}[x]$

c) $(1 + i)[(1 - i)x^2 + x - i]$

d) $\sqrt{2}[\sqrt{2}x^2 + (\sqrt{2} - 1)x + 2\sqrt{2}]$

**40.** a) $(2x^2 + 3x + 36)$

b) $[x^2 - 5(1 + i)x + 4]$

c) $\dfrac{1}{-4 + 4\sqrt{2}}[(-1 + \sqrt{2})x^2 +$

$+ (2 + 2\sqrt{2})x + \sqrt{2}]$

# ÍNDICE REMISSIVO

## A



## B



## C

## D



## E

## F





## G



## H

## I



## J



## K



## L



## M



## N

## O



## P



## Q



## R

# BIBLIOGRAFIA



ABRAMO, H. *Curso de álgebra*. Rio de Janeiro: Impa, 1993. v. 1.

ALEKSANDROV, A. N. et alii. *La matemática, su contenido, métodos y significado*. Trad. para o espanhol por Manuel López Rodriguez. Madrid Alianza, 1974. 3 vol., v. 1.

AZEVEDO, A. *Introdução à teoria dos grupos*. Rio de Janeiro: Impa, 1969.

BARBOSA, R. M. *Elementos de lógica aplicada ao ensino secundário*. São Paulo: Nobel, s. d.

BIRKHOFF, G. e MACLANE, S. *Álgebra moderna*. Trad. para o espanhol por Rafael Rodriguez Vidal. Barcelona: Teide, 1954.

BOYER, C. B. *História da matemática*. Trad. por Elsa F. Gomide. São Paulo: Edgard Blücher, 1996.

BURTON, D. M. *Abstract and linear algebra*. Reading, Massachusetts: Addison-Wesley, 1972.

CASTRUCCI, B. *Elementos de teoria dos conjuntos*. São Paulo: GEEM, 1972.

COUTINHO, S. C. *Números inteiros e criptografia*. Rio de Janeiro: Impa/SBM, 2000.

DEAN, R. A. *Elements of abstract algebra*. New York: John Wiley & Sons, 1967.

DOMINGUES, H. H. *Fundamentos de aritmética*. São Paulo: Atual, 1998.

——, IEZZI, G. *Álgebra moderna*. 3. ed. São Paulo: Atual, 2000.

DONEDDU, A. *Cours de mathématiques supérieures*. Paris: Dunod, 1996. 4 vol., v. 1.

DURBIN, J. R. *Modern algebra*. New York: John Wiley & Sons, 1979.

EVES, H. *Introdução à história da matemática*. Trad. por Hygino H. Domingues. Campinas: Editora da Unicamp, 1995.

FRALEIGH, J. B. *A first course in abstract algebra*. Reading, Massachusetts: Addison-Wesley, 1967.

GOMES, A. M. *Introdução à álgebra moderna*. Rio de Janeiro: Faculdade Nacional de Filosofia, 1960.

IEZZI, G. *Fundamentos de matemática elementar*. São Paulo: Atual, 1993. 10 vol., v. 6.

KATZ, V. *A history of mathematics*: an Introduction. New York: Harper-Collins, 1992.

KOULIKOV, L. *Algèbre et théorie des nombres*. Trad. para o francês por Oleg Partchevski. Moscou: Mir, 1982.

LANG, S. *Estruturas algébricas*. Trad. Claúdio R. W. Abramo. Rio de Janeiro: Ao Livro Técnico/MEC, 1972.

LIMA, E. L. et alii. *A matemática do ensino médio*. Rio de Janeiro: SBM, 1996. 3 vol., v. 1.

MACLANE, S., BIRKHOFF, G. *Algebra*. New York: Macmillan Publishing; Londres: Collier Macmillan Publishers, 1979.

MONTEIRO, L. H. J. *Elementos de álgebra*. Rio de Janeiro: Livros Técnicos e Científicos/Impa, 1974.

MURAKAMI, C. *Fundamentos de matemática elementar*. São Paulo: Atual, 1993. 10 vol., v. 1.

NACHBIN, L. *Introdução à álgebra*. Rio de Janeiro: McGraw Hill/Brasília: Editora da UnB, 1971.

ORE, O. *Number theory and its history*. New York: McGraw Hill, 1948.

PASSMAN, D. S. *Permutation groups*. New York: W. A. Benjamin, 1968.

PERLIS, S. *Introduction to algebra*. Waltham, Massachusetts: Blaisdell, 1966.

STANTON, R. G., FRYER, K. D. *Topics in modern mathematics*. Englewood Cliffs: N. J. Prentice-Hall, 1964.

WAERDEN, B. L. van der. *Modern algebra*. 2 vol., v. 1. Trad. para o inglês por Fred Blum. New York: Frederick Publishing, 1943.

WEISS, M. J., DUBISCH, R. *Higher algebra for the undergraduate*. New York: John Wiley & Sons, 1962.

# ÁLGEBRA MODERNA

Hygino H. Domingues
Gelson Iezzi

Inteiramente reescrita e ampliada, a presente edição de *Álgebra moderna*, dos professores Hygino H. Domingues e Gelson Iezzi, ajusta-se mais adequadamente às atuais tendências do ensino universitário de matemática. Entre outras características, a linguagem é menos simbólica e formal que a das edições anteriores e o conteúdo é muito mais rico em exemplos e ilustrações. Há também uma série de notas históricas que contam as origens dos vários tópicos abordados. As listas de exercícios foram reelaboradas e enriquecidas, visando a uma integração maior com a teoria.

O conteúdo abrange os seguintes tópicos:

- Conjuntos e demonstrações
- Aritmética dos números inteiros
- Relações, aplicações e funções
- Grupos
- Anéis e corpos
- Anéis de polinômios
- Anéis fatoriais